The Year 2000 Problem and Government Procurement

This paper discusses the Year 2000 (Y2K) Problem--the two-digit year format used in computers--as it relates to federal government information technology (IT) buys. The scope is limited, focusing on the regulatory and legislative efforts to minimize Y2K impacts as the government buys commercial and non-commercial IT supply items. Following a brief introduction, the paper surveys the Y2K background, including the nature and genesis of the Year 2000 Problem, its scope and magnitude, some of the technical solutions, and several remediation issues. The bulk of the paper deals with the General Services Administration Year 2000 Warranty clauses and the Federal Acquisition Regulation Year 2000 compliance provisions, analyzing the warranty and regulatory provisions and determining the adequacy of their coverage. The most important focus of the paper is on embedded technology--meaning IT that has been integrated into a product whose nature or purpose is such that the product is not itself considered IT--and the government's failure to address embedded IT. The paper concludes with other governmental efforts to address Y2K, both attempted and still optional, ending with a few recommendations.

Author: Major Brent Curtis
Thesis: in fulfillment of the LL.M. in Government Procurement Law at
The George Washington University School of Law

19990805 093

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 24.Jun.99	3. REPORT TYPE AND DATES COVERED THESIS

4. TITLE AND SUBTITLE GOVERNMENT PROCUREMENT AND THE YEAR 2000	5. FUNDING NUMBERS

6. AUTHOR(S)
MAJ CURTIS BRENT G

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) GEORGE WASHINGTON UNIVERSITY	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) THE DEPARTMENT OF THE AIR FORCE AFIT/CIA, BLDG 125 2950 P STREET WPAFB OH 45433	10. SPONSORING/MONITORING AGENCY REPORT NUMBER FY99-137

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT Unlimited distribution In Accordance With AFI 35-205/AFIT Sup 1	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

14. SUBJECT TERMS			15. NUMBER OF PAGES 159
			16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

GOVERNMENT PROCUREMENT AND THE YEAR 2000

By

Brent G. Curtis

B.S. May 1980, Bob Jones University
J.D. May 1992, University of Dayton School of Law

A Thesis submitted to

The Faculty of

The George Washington University
Law School
in partial satisfaction of the requirements
for the degree of Master of Laws

January 31, 1999

Thesis directed by
Frederick J. Lees
Professor of Law

1

GOVERNMENT PROCUREMENT AND THE YEAR 2000

B. Curtis

B. Curtis

GOVERNMENT PROCUREMENT

AND

THE YEAR 2000

"As the world's leading consumer of information technology (IT) products and services, the Federal Government may well become, if it is not so already, the biggest victim of an impending IT disaster known as 'the Year 2000 problem.'"[1]

I. INTRODUCTION

The Year 2000 Problem, also known as the Millennium Bug, Century Date Change, Date Rollover Problem, or simply Y2K,[2] is a label for what has become a collection of problems that result from the way in which computers have been designed and programmed over the years. The most significant issue, and the one most clearly identified as the Year 2000 Problem, is the predicament posed by the date format which uses only two-digits to represent the year. Because of the two-digit year format, software,[3] hardware,[4] firmware[5] and microchips[6] may be unable to function properly

---

[1] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998).

[2] The "Y" stands for "Year" and the "2K" is shorthand for 2000.

[3] Defined as

> [t]he program and instructions that make up the intelligence of the computer. The term generally is used to refer not only to computer programs but also to the documentation that comes with them. The logic and directions loaded into the machine that causes it to do certain things on command. Software programs include: operating systems; language assemblers, compilers, and interpreters; and utility and application programs.

JAMES V. VERGARI AND VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER--HIGH TECHNOLOGY LAW (American Law Institute - American Bar Association Committee on Continuing Professional Education 1991) at 616.

[4] Defined as "[t]he physical parts of the computer, such as the keyboard, video monitor, printer, and central processing unit; distinguished from software. JAMES V. VERGARI AND VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER--HIGH TECHNOLOGY LAW (American Law Institute - American Bar Association Committee on Continuing Professional Education 1991) at 609.

[5] Defined as "[s] oftware on a chip; programs stored on ROM [(read only memory)] chips, as distinguished from software programs stored on tapes or diskettes. JAMES V. VERGARI AND VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER--HIGH TECHNOLOGY LAW (American Law Institute - American Bar Association Committee on Continuing Professional Education 1991) at 608.

B. Curtis

once they encounter dates later than December 31, 1999.[7] For those computing devices which were designed to use only the last two digits of the year in performing their functions, dates beginning with January 1, 2000 may produce unintended, unanticipated, unwelcome results. The devices may stop operating, produce warnings of erroneous data inputs or otherwise reject legitimate date entries,[8] or produce erroneous results possessing the potential to wreak a havoc whose seriousness is dependent upon the particular function the device was designed to perform. Those who believe the Year 2000 Problem will not affect them because they do not own a personal computer nor use computers in their job are sorely mistaken.[9] The Year 2000 Problem is everyone's problem: there probably is not a single person in the United States (or any developed nation) who will not feel some repercussions from the Year 2000 Problem. The significance of that experience will depend directly upon how much of the problem can be remedied before January 1, 2000.

Within the federal government, the Year 2000 Problem is a both a procurement problem and a problem for IT the government already owns. Numerous facets of

---

[6] Defined as "[a] chip that serves as the CPU that controls a computer." JAMES V. VERGARI AND VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER--HIGH TECHNOLOGY LAW (American Law Institute - American Bar Association Committee on Continuing Professional Education 1991) at 612. The CPU is defined as the [a]bbreviation for Central Processing Unit. The industry name for the main body of the computer; the part of the computer where machine instructions are carried out; the 'brains' of the computer. It acts as an electronic traffic cop handling data signals which come from a keyboard terminal or disk storage drives, controlling the interpretations and execution of program instructions, processing data, and then sending output to its destination. The CPU is the essential core of the computer system, containing the Arithmetic/Logic Unit, Main Memory, and the Control Unit.
Id. at 604.

[7] See GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997), also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[8] The problemsome dates will be from the Year 2000 but will, nonetheless, certainly be proper dates, regardless of whether the particular computer device recognizes or correctly interprets the date.

[9] According to Harris Miller, president, Information Technology Association of America, personal computers (PCs) are susceptible to the Y2K problem in at least three ways: the PC's BIOS chip, the PC's operating system, and the applications software running on the PC. Miller concludes that to accurately operate in the Year 2000, most personal computer systems will need some modification. Statement of Harris Miller, president, Information Technology Association of America, before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight, Subcommittee on Technology, Committee on Science, Solving the Year 2000 Computer Problem, September 10, 1996.

B. Curtis

government procurement will experience the impact of the Year 2000 Problem--some more harshly than others--and each of those facets is significant enough to warrant in-depth research and consideration in the remaining months leading up to January 1, 2000.[10] This paper is limited in scope, focusing on the regulatory and legislative efforts to minimize the impact of the Year 2000 Problem on the federal government, and the people it serves, specifically as government agencies acquire commercial and non-commercial supply items. To date, the government's efforts to avoid procuring items that are not Year 2000 compliant have focused almost exclusively on IT purchases. The two most important developments affecting the government's procurement of Year 2000 compliant IT are the General Services Administration Year 2000 Warranty clauses and the Federal Acquisition Regulation Year 2000 compliance provisions. The paper emphasizes these efforts, analyzing the warranty and regulatory provisions and determining the adequacy of their coverage. The most important focus of the paper is on embedded technology, meaning IT that has been integrated into a product whose nature or purpose is such that the product is not itself considered IT. "Despite the widespread awareness [of the Year 2000 Problem], one of the most challenging and critical manifestations of the problem frequently has been overlooked, understated, and underestimated--the embedded systems problem."[11] Embedded technology represents a large area of the Year 2000 Problem--perhaps the largest--and yet the government

---

[10] Merely as an example, note that the government's ability to engage in electronic commerce may be greatly affected by the Year 2000 Problem. From the computers used to determine and record the government's requirements, through the communications links and data interchanges that those requirements travel across as invitations for bids (IFBs) or requests for proposals (RFPs), to the electronic bulletin boards and the Commerce Business Daily where those IFBs and RFPs are electronically manipulated, posted and published for worldwide availability, to the potential government contractors who will use computer technology to access these postings and formulate and record their bids or proposals, and finally back to the government's systems for receiving, downloading, accessing and evaluating offerors' submissions. Every step of the way, technology plays a part in this "most-favored" contracting mechanism and, while designed to streamline the process, threatens to be the choke-point, denying or delaying the information necessary for the government to fulfill its needs.
[11] David M. Nadler, *Embedded Systems--The Real Year 2000 Problem*, found at http://www.comlinks.com/legal/dnemb1.htm, site visited on December 10, 1998.

B. Curtis

has not given embedded technology sufficient attention in its efforts to regulate the acquisition of non-compliant IT.

Following the Introduction, Chapter Two establishes the Year 2000 background leading up to the government's legislative and regulatory actions. The chapter covers the nature and genesis of the Year 2000 Problem, its scope and magnitude, some of the technical solutions for the problem, and several issues facing the government as it addresses the Year 2000 (Y2K). With that foundation established, Chapter Three shifts the focus to the General Services Administration (GSA), chronicling its efforts to insure that government IT purchases are warranted against Year 2000 problems, and analyzing the features of the Year 2000 Warranty clauses. Chapter Four examines the rules added to the Federal Acquisition Regulation (FAR) to define Year 2000 compliance and limit IT acquisitions to compliant products, noting the effectiveness of those rules and exploring the issues they leave open. Chapter Five addresses the problems posed by embedded technology, noting how and why that segment of IT is not adequately addressed by the FAR, and clarifying several other areas of questionable regulatory coverage. Briefly, Chapter Six surveys other governmental methods of addressing the Year 2000 Problem, both those already employed and those which remain as options. The paper concludes with Chapter Seven: a summary of the issues addressed and a few recommendations.

II. BACKGROUND

A. WHAT IS THE YEAR 2000 PROBLEM?[12]

The "Year 2000 Problem" was initially used to refer to the difficulties that were anticipated when the date function in computer systems rolled over from 1999 to 2000. As attention has focused upon computing systems, additional problems have been

---

[12] The number of new books on the Year 2000 grows daily. A list of over 70 recent titles (as of November 11, 1998) on this topic is found at http://www.year2000.com/y2kbooks.html, site visited on November 11, 1998.

B. Curtis

discovered and a whole range of near and far term computer-related problems have been predicted. Most of these problems are not directly related to the 1999 to 2000 date rollover, yet have been included under the "Year 2000 Problem" umbrella due to their similarity--in cause or effect--to the date rollover problem. Early in 1998, Congress defined the term, simply reversing the Year 2000 compliance definition developed by GSA and the Interagency Committee described in Chapters II and III.

> Section 2.a.(5) the term "Year 2000 computer problem" means, with respect to information technology, any problem which prevents such technology from accurately processing, calculating, comparing, or sequencing date or time data--
> (A) from, into, or between--
> (i) the 20th and 21st centuries; or
> (ii) the years 1999 and 2000; or
> (B) with regard to leap year calculations.[13]

As the scrutiny upon IT intensifies, additional problems will likely continue to surface and be included in discussions of the Year 2000 Problem.

1. *Terminology*

The Year 2000 Problem is often referred to as the "Millennium Bug" and is discussed as though "bug" meant "virus."[14] The "Millennium Bug" is not a computer virus. Typically, a computer virus is a section of computer software code written intentionally to either damage other computer software, corrupt data, disrupt normal computer processing, or take control of the "infected" computer or its peripheral devices when allowed access to another computer system. By contrast, the Millennium Bug is a *condition,* common in many computer systems which store and process date data, that occurred as a result of the date storage convention selected by early computer programmers. The harm from the Millennium Bug, while arguably foreseeable, was

---

[13] Examination Parity and Year 2000 (Y2K) Readiness for Financial Institutions Act, Pub. L. No. 105-164, 112 Stat. 32 (1998).

[14] As an example, a congressional report of hearings on the Year 2000 software conversion correctly identified the two-digit date-field basis of the Year 2000 Problem and then concluded that "[i]f left unchanged, a global computer virus could result." Year 2000 Computer Software Conversion: Summary of Oversight Findings and Recommendations, H.R. Rep. No. 857, 104th Cong., 2d Sess. (1996), para I.B.

B. Curtis

never intended. This two-digit convention for storing the year portion of dates is projected to cause many unintended results as affected computers process date data, much as a computer system infected by a computer virus may produce erroneous results or halt processing operations completely. Some computer viruses are designed to "incubate," coded to cause their damage only after a defined length of time or upon reaching a specified date. Here again, the Millennium Bug is somewhat similar in that the problems associated with this date-handling issue are typically triggered by a date beyond December 31, 1999. So, while there are similarities between what may happen as the result of the Year 2000 Problem and what often happens to an infected computer, the "Millennium Bug" is not a virus.

A more reasonable explanation of the label "Millennium Bug" is the old programming term for software coding errors that were identified as "bugs" in the program.[15] Programming "bugs" were usually errors in logic which directed the computer to function in some way other than that intended by the programmer. This definition of "bug" more accurately approximates the situation described as the Millennium Bug, although most bugs do not take so long to become apparent. Technically speaking, the two-digit date field convention was not really a "bug" when it was written into many software programs. It is only with the passage of sufficient time, as the need to distinguish between centuries has become important, that this programming convention has become a stumbling block to much of the older--and even more current--computer software.

One other semantic difficulty with the term "Millennium Bug," and the general rhetoric surrounding the Year 2000 Problem, is the inaccurate use of the term

---

[15] The term "bug" is widely rumored to have been first used in computer circles when Admiral Grace Hopper, a pioneer in DoD computer science development, was having a great deal of difficulty getting a computer program to process properly. After checking and double-checking the software logic, Admiral Hopper suggested the engineers remove the back panel of the computer system to examine the hardware. Much to the surprise of all, an insect--"bug"--was found inside, and after it was removed, the computer began to function properly. From this incidence, and others like it, came the term "debugging," the process of removing software logic "bugs" that impede accurate processing.

B. Curtis

"millennium." Technically speaking, January 1, 2000 will not be the first day of the new century or the next millennium; rather, it will be the last year of this century and of the second millennium AD.[16] The Twenty-first Century and the Third Millennium actually begin on January 1, 2001. However, in consideration of the language used in discussions of the Year 2000 Problem,[17] references in this paper to "the new millennium," "next millennium," "millennial dates," or similar terms using the word "century" will indicate dates beginning with January 1, 2000.

2. *Two-Digit Year Date Field*

The essence of the Year 2000 Problem is the two-digit year date field. This problem was--and remains--the key issue for the Year 2000, apart from all of the other computer-related issues which have been tossed on the Y2K band wagon as yet another problem associated with the way computers operate or store data. Most computers and computer-related products have been designed to represent the year portion of a date with only two digits. Hardware, software, and firmware marketed or

---

[16] The Year 2000, as a nice round thousand number, will almost certainly be heralded in the print and electronic media as the "new millennium" with, perhaps, an occasional footnote-like reminder that the third millennium actually begins with the first day of the Year 2001. For those whose personal calculations disagree, claiming the next millennium begins January 1, 2000, the Royal Greenwich Observatory provides an authoritative explanation for the millennia question.

A millennium is a period of 1000 years. The question of which year is the first year of the millennium hinges on the date of the first year AD.

Unfortunately the sequence of years going from BC to AD does not include a Year 0. The sequence of years runs 3 BC, 2 BC, 1 BC, AD 1, AD 2, AD 3 etc. This means that the first year of the first millennium was 1 AD. The one thousandth year was AD 1000 and the first day of the second millennium was AD 1001.

It is thus clear that the start of the new millennium will be 1 Jan 2001.

The Year AD 2000, Information Leaflet No. 52, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, May 23, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/2000/2000.html, site visited on September 30, 1998.

[17] Even the president of the United States erroneously describes the Year 2000: "It seems unbelievable that it's only 535 days from now, at the stroke of midnight, when we will usher in a New Year, a **new century**, a **new millennium**." Remarks by the President concerning the Year 2000 conversion, delivered July 14, 1998 at the National Academy of Sciences, and found at http://www.y2k.gov/new/presy2k.html (October 3, 1998), *emphasis added.*

B. Curtis

developed in the United States and abroad is programmed to store a date such as December 7, 1941 as "120741" with the last two digits signifying the year. Date fields with two-digit year identifiers carry an "implied century" which, until now, has always been the twentieth century (1900s). Technically speaking, computer dates will not roll over from "1999" to "2000;" rather, they will roll over from "99" to "00," and that is the essence of the problem. On January 1, 2000, computer systems around the world will function as though time had been robbed of 100 years in a mere instant, returning the world to the Year 1900.

"These two-digit dates exist on millions of data files used as input to millions of applications."[18] Computers use date data in many applications, only some of which are obvious to the end user and even fewer to the typical consumer. Many of these applications process date data by subtracting and comparing dates. A computer in the Social Security Administration would subtract the author's son's date of birth (1985) from the current date (1998) and compare the result to 65 to determine if he were old enough to be eligible to receive full social security benefits. Using only two-digit year fields, the computer's process would subtract 85 from 98, compare the resulting 13 years of age to 65, and deny any request for benefits. If that same system continues to use two-digit year fields in 2000, the computer would subtract 85 from 00, compare the resulting 85[19] to 65, and declare my (then) 15 year old son eligible for full benefits. With this information, people born from 1965 or later might well be lined up to apply for social security benefits on January 3, 2000: the first working day of that year. Those truly entitled to benefits--those born in 1935 or earlier--would actually be deemed ineligible, having been determined by the computer to be 35 years old or younger! This same

---

[18] Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998.
[19] Two-digit systems that process dates in this manner do not typically distinguish between positive and negative numbers, primarily because they were designed under the assumption that this problem would not occur.

B. Curtis

error process will affect any system that uses passages of time to calculate other amounts, such as determining interest payments or amortization tables.

Systems which sort records based upon date will experience the same problem. Computer-generated "date-stamps" can easily distinguish dates/time of day down to a fraction of a second. For the sake of demonstration, assume a group of dates that consisted only of the year portion, such as 1985, 1958, 1991, and 1987. When a two-digit computer sorted these records according to date, the computer would produce the sequence 58, 85, 87, 91. When dates from the next century are added in to be sorted, such as 2525, 2001, and 2081, the computer-produced sequence would be 01, 25, 58, 81, 85, 87, 91. Here, again, the results would be wholly inaccurate and unreliable.

3. *Year 2000 Leap Year*

Another piece of the "Year 2000 Problem" is that the Year 2000 will be a leap year and, due to the obscure nature of the rules used to determine leap years, many computer systems may not have been programmed to anticipate the extra day that will occur in 2000. Most school children can recite the rule that Leap Year comes every four years, and that in such a year the month of February has 29 days instead of 28. The Julian Calendar, established by Julius Caesar in 46 BC, introduced leap years in recognition of the fact that there were approximately 365.25 days in a year.[20] Over time, the difference between the approximate year length (365.25 days) and the actual year length (365.24219 days) began to accumulate.[21] In 1582, Pope Gregory instituted

---

[20] " *Leap Years*, Information Leaflet No. 48, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, April 17, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/leapyear/leapyear.html, site visited on September 30, 1998. Although leap years were included in the Julian Calendar from its creation, they were not correctly inserted into the calendar until 8 AD. *Id.*

[21] " *Leap Years*, Information Leaflet No. 48, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, April 17, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/leapyear/leapyear.html, site visited on September 30, 1998. By the 16th Century, the seemingly negligible difference between the approximate and actual year length had accumulated to several days. *The Year AD 2000,* Information Leaflet No. 52, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, May 23, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/2000/2000.html, site visited on September 30, 1998.

B. Curtis

the Gregorian Calendar, compensating for the lack of precision used to determine leap years by instituting the second leap year rule.[22] Fewer people know this second rule: every hundred years a leap year is skipped, so that the last year of a century--such as 1700, 1800, or 1900--is not leap, even though it is the fourth year following the last leap year. Some, but not all, programmers were aware of this rule and observed it when programming for the number of days in the Year 2000.[23] The third rule, as it is frequently described in Year 2000 Problem discussions, is actually part of the correction formula derived under Pope Gregory. To approximate the actual year length of 365.24219 as precisely as possible, leap year should be skipped on century years only if they are not divisible by 400.[24] Therefore, every four years we have a leap year unless that year ends in "00" *and* is not evenly divisible by 400. Hence, the Year 2000 is a leap year.

Given the fact that these rules have been in existence since 1582, one might presume that computer programmers, who are used to dealing with all sorts of technical details, would likely have taken these rules into account when writing software and properly coded the Year 2000 as a leap year. However, as late as 1997, arguments persisted about whether or not 2000 would be a leap year,[25] and some programmers have yet to master the basic rule of including an extra day in the normal, once-every-

---

[22] *The Year AD 2000,* Information Leaflet No. 52, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, May 23, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/2000/2000.html, site visited on September 30, 1998. Pope Gregory was concerned about this date shift moving the celebration of Christ's crucifixion and resurrection from the Spring towards the time of year that had been December 25th, when the church celebrated Christ's birth. *Id.*

[23] Few computer programmers would have been born--much less been old enough--during the most recently "skipped" leap year (1900) to have had personal memory of the unusual event.

[24] " *Leap Years,* Information Leaflet No. 48, Particle Physics and Astronomy Research Council, Royal Greenwich Observatory, April 17, 1996, found at http://www.ast.cam.ac.uk/pubinfo/leaflets/leapyear/leapyear.html, site visited on September 30, 1998. This formula approximates more closely approximates the actual year length, equating to an average of 365.2425 days per year. The difference between 365.2425-day years and 365.24219-day years will accumulate at a rate close to 1 day each 4,000 years, so that when computers next have to change date field sizes to accommodate dates into the Year 10,000, the calendar will have shifted approximately 2.5 days. *Id.*

[25] Ashley Dunn, *Y2K Bug: Problem for the Ages*, WISCONSIN ST. J., at 1C, August 21, 1998.

B. Curtis

four-years, leap year. In fact, one industrial plant has already experienced a system-wide failure because the system's programmers failed to include a 366th day in 1996, the last leap year.[26] As it turns out, those who were not aware of the special century-year-skipping rules may have programmed for the right number of days in 2000 for the wrong reason.[27]

4. *"9999" Computer Dates*

The digits "9999," which would normally be understood as September 9, 1999 (9/9/99), have been used in many computer programs and data files to represent something other than an actual date.[28] "In fact, most early uses of the digits '9999' used in date fields in early programs and applications meant anything but September 9, 1999."[29] The practice of using nines developed into a programming standard, somewhat in the same manner that the two-digit year date field became a programming convention by programmers repetitious employment of that practice. The digits "9999" have to a large degree become the standard numbers supplied to computers in several situations. "Some programmers used nines as an expiration date for data," indicating that the data should be deleted from the system as obsolete when that date was achieved.[30] This mean that some systems, left uncorrected, may delete data simply because the programmer did not anticipate his work maintaining a useful life beyond the twentieth century. In some of the truly older legacy systems, programmers had added "9999" to the end of data files as a marker to indicate to the processor that the

---

[26] EDWARD AND JENNIFER YOURDON, TIME BOMB 2000--WHAT THE YEAR 2000 COMPUTER CRISES MEANS TO YOU! (Prentice Hall PTR 1998), at 284. This example is discussed in more detail in the section of Chapter V dealing with the problem of omitting embedded technology.

[27] Interestingly, of the various computer problems that have been grouped under the Year 2000 Problem heading, leap year is the only "other" Year 2000 problem which was addressed in the GSA Year 2000 Warranty clauses and the FAR's Year 2000 Compliant definition.

[28] "Unlike the year-2000 bug, the Sept. 9 snag is not about computers assuming it's 1900 when reading a two-digit date. It has the same root though: Programmers failing to anticipate the future." Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7.

[29] Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7.

[30] Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7.

B. Curtis

file end had been reached and the processing could halt and move to the next file.[31] In this situation, the application program may improperly omit or fail to process portions of data files after encountering a 9/9/99 date and wrongly determining that the numerals indicate the end of the file has been reached.[32]

The "9999" digits are also used when an actual date is either unknown or indefinite. Both in programming and in everyday computer operations, situations arise when a computer system requires a date be submitted and sometimes there is no certainty about what that date should be at the point when it is demanded. In such instances, the practice has become routine to supply nines as a "dummy" date which fills the required field, but does not attempt to represent a true date.[33] Computer users may input "9999" when they do not know what date should be input for one of several reasons: 1) because that date will stand out on any future report, bringing the entry to their attention so they may supply the proper date, assuming it has become known; or 2) because the system will not allow the operator to proceed without supplying a date, and "9999" is an easy set of digits to enter quickly.[34]

For instance, consider a programmer designing a software application for database management who wants the system to automatically archive older information at some point in the future. Because the programmer cannot predict when circumstances will be at optimal for performing the archival routine, the date is unknown and the programmer codes a 9999 into the date field. Once the system is delivered, the system manager can determine the best schedule for archival processing and supply a date to the system. If the system manager has scheduled the archiving by

---

[31] *See* Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7.

[32] *See* Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7.

[33] The obvious problem is that "9999" does represent a true or actual date, although one which seemed sufficiently distant when the practice first began.

[34] For much the same reasons, some people who perform data entry requiring Social Security Administration Numbers will enter "999-99-9999" when they do not actually have or know the number that should be supplied to the system.

B. Curtis

supplying a specific date, no problem will occur because the 9999 will have been overwritten with the optimal date. Where those 9999 date fields remain, archival operations will be initiated on September 9, 1999 much to the surprise—and possibly disappointment—of those affected by the untimely operations.[35]

In other situations when a computer user is asked to supply a date, the date requested is not an unknown date, but an indefinite date. The distinction is the difference between the undetermined but definite date when something will take place (unknown) and a date which may never come (indefinite). Sometimes when a software application demands a date, the only certainty is that the date supplied should be somewhere in the future. In such circumstances, programmers and operators commonly picked "9999," a "distant future" date, or at least one that was easy to input. As an example, a security system might demand a start and end date for personnel authorizations so that registered persons would be permitted access to a secure facility only within the dates prescribed. Where a person's access was expected to continue for years with no projected termination date, security managers might input the indefinite 9999 rather than some actual date.[36] The fact that 9999 is, in fact, an actual

---

[35] The archival illustration is merely one, relatively passive operation that might be unintentionally initiated on September 9, 1999. Where 9999 has been coded into systems which perform more critical functions, the results could be far more serious. What if 9999 were coded into the override system at a prison facility so that all cell and corridor doors could quickly be opened in the event of an emergency evacuation. What if the inventory control system at a large storage facility automatically inserts 9999 into the computer for the expiration or destruction date for stored items when the actual date is not known. Given the longevity of some of the software systems in operation today and the firmly established practice of supplying this "dummy" date for unknown and indefinite dates, it is not too difficult to imagine serious situations which may occur on September 9, 1999 for those who do not examine their systems and make necessary changes prior to that date.

[36] Security managers could, and in some cases should, enter expiration dates limiting access to a predetermined number of months or years. This would require a continuing review and update process: 1) which persons are approaching the "access-denied" date, 2) of those, who should continue to have access, and 3) update the access termination date for those users. Low security operations and other information tracking systems would not benefit from the additional administrative burden of such a review and update process. As a further example, any service or organization could offer a lifetime membership which could be opened with a fixed starting point but an undetermined ending point. Selecting 9999 as the indefinite ending date for the membership made sense 10 or 20 years ago, but anyone whose record has not been updated before September 9, 1999 will find themselves "former members" in spite of their longevity.

B. Curtis

date will become stunningly apparent on September 9, 1999 to those who have used that designator as a dummy date when they were not able to determine the date which would best meet the application's purposes.

The "9999" computer date is not truly a century-date problem. Whether the last two digits are deemed to belong to the 1900s or the 2000s, the problem remains. That is to say that the transformation or migration from a two-digit to a four-digit year date field will not correct this problem. If a system has been coded to take a particular action on September 9, 1999, it will take that action whether the system reads the date as 9/9/99 or 9/9/1999. Therefore, even systems which are Year 2000 compliant may produce unanticipated results on September 9, 1999 if the system was coded to perform certain operations and "9999" was supplied as the action-triggering date.[37] This problem must be fixed *even earlier* than the Year 2000 deadline of January 1, 2000.[38]

5. *Data Overflow*

Two types of data overflow can occur. One happens when the particular field designated to store data is exceeded by the length of the data that is input to that field. In short, its like trying to put thirteen eggs into a regular "dozen-sized" egg-carton. For example, data overflow may occur when attempting to supply a date containing a four-digit year (e.g. July 8, 1991, input as 07081991) into a data field designed to store dates in two-digit year format (e.g. July 8, 1991, stored as 070891). Depending upon

---

[37] The only problem that might be avoided in systems which have been made Year 2000 compliant is the mistake of reading nines as an end of file indicator. If the date is changed to a four-digit year field, there would no longer be a date in the file that would be "9999,"[37] so that September 9, 1999 would be read as "991999 and would not trip the end of file indicator.

[38] As with the century-date portion of the Year 2000 Problem, no one truly has the final answer on how great a problem is posed by the 9999 dates. "Both Cap Gemini's Mr. Woodward and Barry Ingram, vice president and chief technology officer for EDS, say they expect the 'nines' fallout to be relatively minor." Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998, at A1, A7. Mike Humphrey, of Public Technologies Inc., has a different perspective on the problem posed by 9999 dates: if the breakdowns of January 1, 1999 (for 12-month, forward-looking systems) and September 9, 1999 are not very significant, "computer users might dismiss the year-2000 issue as hype and hysteria and halt expensive repairs months before the big problems predicted by many experts on Jan. 1, 2000." *Id.*

B. Curtis

the software and any error handling routine programmed into it, the date may be truncated to the first six digits (which will be stored, processed, and retrieved as July 8, 1919), or truncated to the last six digits (which will be stored, processed, and retrieved as August 19, 1991),[39] or the system might reject the entry as not properly formatted.[40] Whatever the result, the proper date data has not been stored in the field.

The second type of overflow occurs when a "counter" reaches the end of its boundaries and rolls over to zero and continues counting, much like a car whose odometer reaches the final series of nines (all digit places reading "9") and then returns to zeros. When the counter rolls over to zeros, it is said to have overflowed. This can occur in hardware which calculates the current date or time by adding an offset (of days, hours, minutes, seconds and possibly microseconds) to a fixed reference point that has been programmed or "hardwired" into the hardware. As an example, most personal computers allow the user to input the date and time. This entry establishes the offset for the processor so that every function thereafter which uses date or time can be determined by adding the offset (the amount of time which has passed since the user last supplied the date and time) to the current time as tracked in the computer's clock. If the clock register has an upper limit, then when that number is exceeded the data overflows and the results are unpredictable. Even where the date and time are not reported, data overflow may cause spurious results if the date/time data is used in calculations.

Data overflow is not uniquely a Year 2000 problem; rather, it is just one example of what has been termed "bounded storage." In essence, bounded storage is just another way of saying that all computers are finite and can hold, process, report a finite

---

[39] Note that the date December 25, 1998 would have been entered as 12251998 and first-digits truncation would have yielded a date of 25/29/98. Not only would this date have been wrong, just as the other truncated dates would have been incorrect, but because the month indicated is outside the range of possible numbers, this entry might cause a software failure.

[40] This result would actually be the best one might hope for as it would prompt the user as to the existence of a data format problem.

B. Curtis

amount of data. Examples of bounded storage abound. The UNIX operating system, developed by AT&T Bell Laboratories, counts in seconds and use a 32-bit register as the counter.[41] Therefore, the register will overflow at precisely 2^{31} seconds (4 1/4 billion seconds)after the UNIX initiation date (1 January 1970).[42]

Technically speaking, fixing the Year 2000 Problem by creating a four-digit year date field (or any size, for that matter) creates the same data overflow problem as did using the two-digit field for the last 50 years. It sounds ludicrous for us to even be considering the date change from December 31, 9999 to January 1, 10000, much less

[41] *See* Bill Burke, *Second Y2K-like failure set to strike UNIX systems,* BUSINESS TODAY, October 20, 1998, found at http://www.businesstoday.com/techpages/y2kunix080898.htm, site visited on October 27, 1998. "The Year 2000 computer problem may only be a dress rehearsal for a little-known, larger and more widespread computer glitch that could send all mission-critical systems crashing 40 years from now." *Id.* In fact, "the UNIX
glitch is likely to be on par with the coming Y2K problem." *Id. citing* David Cyganski, professor at Worcester Polytechnic Institute. Several years after the operating system was developed, UNIX was provided to researchers and students and had been used, among other things, to develop the Internet's communication software protocols. *Id.*

[42] Bill Burke, *Second Y2K-like failure set to strike UNIX systems,* BUSINESS TODAY, October 20, 1998, found at http://www.businesstoday.com/techpages/y2kunix080898.htm, site visited on October 27, 1998. UNIX developers selected the first second of Jan. 1, 1970 as the fixed reference date, sometimes called "Time Zero." *Id.* Burke points out that UNIX is the operating system for the Internet, most financial systems, and the airlines, all of which may fail in 2038. He notes that several other "tripwire" dates: "Some old Macintosh systems are set to fail in 2040, the IBM 3070 clock will fail in 2042, and in 2005, older 16-bit versions of UNIX will die." *Id. See also* Nicholas Zvegintzov, *The Year 2000 as Racket and Ruse,* first published in AMERICAN PROGRAMMER, February 1996, and now found at http://www.softwaremanagement.com/References/year_2000.html#ruse, site visited on October 21, 1998. The overflow will occur at 03:14:08 on 19 January, 2038. *Id.* After pointing out that the UNIX date is a "bounded storage," Zvegintzov proceeds to enumerate others:
So is the problem of The Bank of New York when it lost track of $25 billion of government securities in the middle of the night because its software handled one more transaction than it was ready for. So is the U.S. Government running out of Social Security Numbers or the telephone company running out of area codes. So is many an unrecoverable application error relating to memory management and memory leak (and many more obscure and dangerous failures). So is the timing error in the Patriot missile launcher that let a Scud missile hit the Dhahran Barracks.
Obviously, data overflow is not limited to date data. Another data overflow situation being discussed in Y2K-related e-mail is described as "D10K." As the story goes, if the Dow Jones Industrial Average reaches 10,000 points, the four-digit system will overflow and not be able to recognize the fifth digit. The exciting portion of the story is what that overflow would trigger: a massive "sell" of stocks, bonds, or any other instruments traded over the Dow. Whether the rumored selling would truly occur or not, the computers used to record and track prices and the average for the Dow has bounds, and if those bounds are exceeded, unintended and probably undesirable results will follow. Appendix A to the DoD Management Plan contains a list of critical dates which should be tested to ensure Y2K compliance and avoid problems after and even before January 1, 2000. DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998.

B. Curtis

worrying about it at this point. Such long-sighted worries are currently the subject of jokes among computer programmers and engineers.[43] However, that is precisely the attitude that existed amongst computer pioneers who began the legacy we are now frantically trying to change.

B. How Did the Problem Come About

"Since the beginning of the information age [circa 1950] no standardized calendar date format has been used--more than twenty formats have evolved, most of which do not accommodate the century change.[44] Stated in its most simple form, the Year 2000 Problem is the result of economy and shortsightedness. Comparing the currently available technology with the technologically austere environment in which the computer programming pioneers operated, it is hard to imagine the lengths to which they were forced to go to economize as they practiced their art. Additionally, it is not too difficult to understand how those pioneers, blazing a trail into uncharted territory, may not have been able to appreciate how the practices they employed would be forged into patterns that would last half a century[45] and lead to the problems we face today. The Year 2000 has been aptly referred to by the president as a "design flaw in millions of the world's computers"[46]

---

[43] Ashley Dunn, *Y2K Bug: Problem for the Ages*, WISCONSIN ST. J., at 1C, August 21, 1998. "No doubt about it . . . . They'll have 8,000 years to figure it out, and still mess up." *Id. quoting* Jerald Hermes, the Year 2000 Strategies Director for a software development/maintenance company which focuses primarily on large, mainframe computers.

[44] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) at 1, parenthetical in original.

[45] *See The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and Governments,* World Information Technology and Services Alliance White Paper, found at http://www.itaa.org/witsay2k.htm, site visited on October 21, 1998. "The Year 2000 computer problem is the single biggest challenge facing the IT industry since the first computer became operational 51 years ago." *Id.*

[46] Remarks by the President concerning the Year 2000 conversion, delivered July 14, 1998 at the National Academy of Sciences, and found at http://www.y2k.gov/new/presy2k.html (October 3, 1998).

B. Curtis

1. *Memory Conservation*

When computer technology was first emerging, and even through its first decade, data storage and resident memory were very expensive.[47] The practical and physical constraints on computer memory led to a particular software programming convention where only two digits were used to identify the year of any particular date data. A date such as March 24, 1958 was stored as 032458, rather than 13241958. Although the difference between the two formats seems practically negligible by today's standards, it is precisely this sort of tedious conservation of precious space resources that was required of early programmers. This sort of economy is not unlike the production of forms which pre-print the first two digits of the year and merely leave the last two digits for the applicant to provide. In addition to conserving memory, using two-digit year fields reduced the number of keystrokes required for operators to enter data and the number of columns required to enter date data when computers were initially programmed via 80 column punch cards.

As computer technology continued to develop, memory and space considerations became less important. Over the years, both data storage, in the form of disk space, and resident memory space, expressed as random access memory (RAM) has expanded with technological refinements and has become much more affordable. Such relative luxury for later software programmers has allowed them to focus more on getting the programs written and less on how many commands and space they consume in doing so. Regardless of what other flexibilities may have entered the software programming environment, the six-digit date field, with two-digit year designators--has remained the standard. Whether for compatibility with earlier software, or because of the other factors discussed below, the two-digit year field has

---

[47] Testimony of Kevin Schick, research director, The Gartner Group, before a hearing of the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight, "Is January 1, 2000 the Date for a Potential Computer Disaster?" April 16, 1996, p. 8.

B. Curtis

become a near-universal convention in the computer world. It is that universality that helps to explain the scope and magnitude of the Year 2000 Problem we face.

2. *Cultural Norm*

Rather than taking the easy route of simply blaming the computer programmers who, for reasons which appeared sound at the time, programmed computers using only two digits to represent the year, some recognize that the date problem is more a matter of how each generation thinks of itself. Unless one was born near the turn of a century, a person easily grows into the pattern of thinking only in terms of which year *within the century* it is. Even close to the end of a century, life spans and the events we experience and discuss are not often so far into the past or future that it is necessary to identify the century in order to be understood. How many forms has the average person filled out during his lifetime that gave only six empty boxes for the date to be filled in, assuming the century and only requiring the last two digits. Earlier forms made the assumption even more explicit, leaving a space for month, day, and then printing "19__" for the year. These forms demonstrate the same assumption that programmers made: this edition of the form (software) will only be used for so many years. Forms and software are not the only place where this cultural norm is evident.

The principle of how pervasive this way of thinking is in our society can best be demonstrated by a brief anecdote.[48] During the Question and Answer period following a Y2K presentation, a lecturer was pompously asked how this problem could have occurred with all of the brain power behind the computer technology and software explosion. Rather than provide any of the standard explanations, the lecturer addressed the questioner, asking what year the gentleman had been born, to which he immediately replied "fifty-eight." "That is precisely why we have the 'Year 2000' problem," stated the lecturer. Our society almost uniformly expresses years in two

---

[48] This story is paraphrased from one listed on-line by Dave Bettinger, Co-leader, SIM Year 2000 Working Group, e-mail address <bett@clinic.net> (copy on file with author).

B. Curtis

digits, and the impact of this cultural norm, more so than any shortsightedness of the computer industry, should not be underestimated in considering how we came to face the present problem. It is the context of any situation which--for people--typically makes it unnecessary to identify the century along with the specific year. When someone describes the year they were born, bought their first car, graduated from school, married, started with a company, or had bypass surgery, the appearance of the speaker is sufficient to establish the century to which the years belong. Computers, however, do not work within such a framework;[49] instead, they merely manipulate and process date data much like any other numeric data, and all assumptions regarding centuries are written into the software or hardware.

3. *Greater Than Expected Software Longevity*

Furthermore, those who created software programs using only two-digit fields to express the year had no idea their programs would be used for a decade, let alone into the next century.[50] Over the years, many software programs have been kept in use by updating and adapting them and even migrating them from one computer system to another. Throughout that process, the two-digit date field was most often preserved, taking the two-digit date field closer and closer to the 20th century where the truncated century digits would be necessary. If programmers from decades gone by had known that the code they were writing would still be running on systems today, they may have

---

[49] This is not to say that computer technology and programming languages are not sufficiently developed to be able to assess a context and determine an appropriate century. While artificial intelligence may present the ability to make the same logical connections we take for granted in such situations, that type of "reasoning" has not been included in most computer systems.

[50] *See generally* YEAR 2000 COMPUTER SOFTWARE CONVERSION: SUMMARY OF OVERSIGHT FINDINGS AND RECOMMENDATIONS, H.R. REP. NO. 857, 104th Cong., 2d Sess. (1996). Those who would criticize programmers for taking such a shortsighted view in designing data structures would do well to remember that it was over 50 years ago that the first computer became operational. *The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and Governments,* World Information Technology and Services Alliance White Paper, found at http://www.itaa.org/witsay2k.htm, site visited on October 21, 1998. Very few people, particularly in our fast-moving environment where even cameras and watches are disposable, would anticipate that anything they create today will still be operating usefully 10 years from now, much less 20 or 30 years.

B. Curtis

taken a more long-sighted view in their drafting and given more attention to creating code which would stand the test of time rather than meeting only the most pressing, present requirements.

4. "Silver Bullet" Assumptions

Given the pace at which computer technology was advancing, many computer experts both in the government and the private sector believed that the continuing advancement would always be able to provide a "silver bullet" solution to whatever problem or technical hurdle that popped up in the pathway of progress.[51] In fact, the process of converting a two-digit date field into a four-digit date field is not a technically challenging one; rather, the tedious (and costly) challenge stems from the complex process of inventorying, converting, testing, and integrating the software and hardware within, among, and between an industry's or the government agency's IT systems.[52] The more technologically connected we become as a society, the more dependent we become one each other's systems.

Apparently some people have such a high regard for Microsoft, in its position of near (if not actual) world-wide dominance over the PC market, that they are looking to the software mega-giant to provide the antidote to the Millennium Bug's bite. One writer "was stunned when an end user told me Bill Gates would probably solve the year 2000 problem soon. At first I thought he was joking, but he was serious."[53] Peter de Jager,[54]

---

[51] *See generally* YEAR 2000 COMPUTER SOFTWARE CONVERSION: SUMMARY OF OVERSIGHT FINDINGS AND RECOMMENDATIONS, H.R. REP. NO. 857, 104th Cong., 2d Sess. (1996).

[52] *See generally* YEAR 2000 COMPUTER SOFTWARE CONVERSION: SUMMARY OF OVERSIGHT FINDINGS AND RECOMMENDATIONS, H.R. REP. NO. 857, 104th Cong., 2d Sess. (1996).

[53] William Ulrich, *Microsoft Offers Little Year 2000 Help*, COMPUTER WORLD, Vol. 33, June 22, 1998.

[54] For over 6 years, de Jager has been busy warning IT and business communities around the world about the impending disaster in the Year 2000. He has published numerous articles (including *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998) and co-authored a book (MANAGING 00) on the subject and has appeared on television news magazine programs and science specials both in the United States and his home country, Canada. De Jager has addressed this issue before the governments of Canada and the United States, as well as the World Economic Forum, and currently serves as special advisor to several government task forces. He created The Year 2000 Information Center on the Internet, manages the Year 2000 mail list (which serves as a virtual discussion group), and speaks on this issue around the

a leader in Year 2000 awareness issues who has been referred to as "the Paul Revere of the Year 2000,"[55] has encountered the same misguided view of Microsoft--as though Bill Gates were some type of messianic figure to the computer technology world--from reporters questioning him regarding the Year 2000 Problem.[56] Some Microsoft product users suspect otherwise about Bill Gates ability to save us all from the Year 2000 problems, having encountered snags in Microsoft's SQL Server.[57] Microsoft acknowledges that the Servers Enterprise Manager does not account for 2000 being a leap year, so operators are unable to schedule jobs on February 29, 2000. Furthermore, the date checking function in its database backup will not operate correctly after January 1, 2000. This defect will allow the backup routine to overwrite older backup media with the material currently being backed up without prompting operators with the standard "Do you really want to do this?" warning. Apparently Bill Gates has not fired his silver bullet yet.

C. SCOPE AND MAGNITUDE OF THE YEAR 2000 PROBLEM

"The Year 2000 computer problem is the single biggest challenge facing the IT industry since the first computer became operational 51 years ago."[58] "With millions of hours needed to rewrite billions of lines of code and hundreds of thousands of

globe. A brief biography covering de Jager's experience regarding Y2K problem awareness is located at http://www.year2000.com/y2kbio.html, site visited on October 21, 1998.

[55] Jay Golter and Paloma Hawry, *Circles of Risk*, found at http://www.year2000.com/archive/NFcirclesrisk.html, site visited on September 15, 1998.

[56] Peter de Jager, "Dear Mr. Gates (Open Letter to Microsoft CEO Bill Gates on Year 2000 Crisis)," Datamation, August 1, 1997, Vol. 43, No. 8. De Jager asks Gates to disavow these reporters, and people around the globe generally, of these silly notions and provide desperately needed leadership by publicly stating that '[n]o silver bullet is possible' and '[a]ll companies are at serious risk and must solve this Year 2000 problem in time.' *Id*.

[57] *See* Timothy Dyck, *Y2K-Proofing Your Databases*, PC WEEK, October 19, 1998, found at http://www.zdnet.com/pcweek/stories/news/0,4153,360733,00.htm, site visited on October 27, 1998.

[58] WORLD INFORMATION TECHNOLOGY AND SERVICES ALLIANCE (WITSA) WHITE PAPER, *The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and Governments,* found at http://www.itaa.org/witsay2k.htm, site visited October 21, 1998.

B. Curtis

interdependent organizations, this is clearly one of the most complex management challenges in history."[59]

1. *Reality of the Problem*

The problem is real. The prospect of problems associated with computer clocks around the globe mistakenly treating the Year 2000 as the Year 1900 has generated two distinct--and somewhat rival--camps. Year 2000 specialists, consultants, and vendors are fairly convinced that serious consequences are fully possible; while Year 2000 researchers and some corporate officers are equally convinced the potential for problems has been greatly exaggerated beyond the relatively minor fallout which may actually occur.[60] One journalist epitomized the skeptical view:

> Legions of so-called Y2K consultants and specialists are already busy raking in millions on the premise that computers will go into gridlock when the clock strikes midnight on Dec. 31, 1999 and the machines are unable to recognize the new '00' code. And all because a few early computer nerds lacked the foresight to account for the possibility of a century change when they designed the first models. And what are the chances that [the Year 2000] technological apocalypse will actually take place and send us back to the age of the slide rule and the abacus? Oh, about the same as the odds that an asteroid from space will hit Godzilla and save New York from destruction.[61]

---

[59] Remarks by the President concerning the Year 2000 conversion, delivered to the National Academy of Sciences (July 14, 1998), and found at http://www.y2k.gov/new/presy2k.html, site visited on October 3, 1998.

[60] Capers Jones, *Probabilities of Year 2000 Damages*, (February 26, 1998), found at http://www.year2000.com/archive/NFproby2k.html, site visited on October 21, 1998. Jones is the Chairman of Software Productivity Research, Inc., located in Burlington, Massachusetts.
'No one wants to step up to the issue - not [IS] management, not the vendors, not the industry gurus,' Orr says. 'As with all legacy systems, this problem is messy, expensive and unromantic. No one wants to go in and tell management they have a multi-million-dollar requirement just to keep the business running and that they really have no options.'
Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998, *quoting* Ken Orr, principal at the Ken Orr Institute, who surveyed corporations and made remediation cost estimates of Fortune 50 corporations. *Id.*

[61] Bill Schadewald, *Bull Market: A crash course in 'catastrophobia,'* HOUSTON BUSINESS JOURNAL, June 1, 1998. Schadewald includes the Year 2000 as part of what he terms "a severe case of collective 'catastrophobia'" the country is suffering from. *Id.* Within two short weeks, after performing some research on the Y2K topic, this same author confessed to having an "overly cavalier attitude toward the ominous implications of Y2K," reversed his position, and admitted that "the chances this technological apocalypse will actually take place . . . are infinitely greater than the odds that an asteroid from space will

B. Curtis

Another journalist cited a Cap Gemini America survey, updated in July of 1998, which "found that 40% of companies polled have already experienced some type of year 2000-related disruption."[62]

Still others see the Year 2000 issue as a "ruse" used by software programmers to get the attention of those who hold the purse strings and so rarely loosen those strings for the cause of software maintenance. The only difficulty with this hyped method of "get[ting] resources where they can . . . for tools and training and preventive maintenance--for more important and difficult software problems" is that managerial "ignorance" will survive the Y2K issue and so the "real problems of software" will remain when the Year 2000 problem has come and gone.[63]

Government agencies and major corporations would not be pouring hundreds of millions of dollars into fixing a nonexistent problem. The Washington Times reported that General Motors has established a contingency reserve approaching $500 million to cover the costs of Y2K compliance, and that the second-largest U.S. bank, Citibank, anticipates spending $600 million preparing its systems for the Year 2000.[64] When Evan Hand, an engineer with Kraft Food, Inc.,[65] spoke at a Y2K conference in Houston about his company's experience, he made it clear that the problem was real, at least to

---

hit Godzilla and save New York from destruction." Bill Schadewald, *Bull Market: Confessions of a Y2K Convert*, HOUSTON BUSINESS JOURNAL, June 15, 1998.

[62] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998. The survey of 128 executives is ongoing and has reported problems including "processing errors, financial miscalculations and customer-service disruptions." *Id.*

[63] "THE YEAR 2000 AS RACKET AND RUSE," Nicholas Zvegintzov, first published in American Programmer, February 1996, and now found at http://www.softwaremanagement.com/References/year_2000.html#ruse (October 21, 1998).

[64] Robert L. Simison, *Year 2000 Problem Could Cost General Motors $500 Million*, THE WALL STREET JOURNAL INTERACTIVE EDITION, March 23, 1998.

[65] Kraft Foods, Inc., the North American food business of Philip Morris Companies Inc., has been in business for over 200 years and traces its history to three of the most successful food entrepreneurs of the late 19th and early 20th centuries: J.L. Kraft (cheese), Oscar Mayer (meats) and C.W. Post (cereals). Today, Kraft is the largest U.S.-based packaged food company in the world. http://kraft.neog.com/careers/scoop/general.html, site visited on October 21, 1998.

B. Curtis

one of the world's largest food conglomerates. He explained how one of Kraft's warehouse processing systems had destroyed several million dollars worth of food labeled with expiration dates after the millennium because the system read the two-digit date code and determined the food had already "expired."[66] Although there are likely many other anecdotal accounts of mistakes, inaccuracies and failures caused by Year 2000 problems,[67] companies are wary of publishing or sharing those examples because of the potential for harm to stock prices and the litigation specter looming large on the millennial horizon.[68]

In fact, the Year 2000 problem has already had an impact on industry and the surrounding culture.[69] Federal and state agencies are swimming up the same stream alongside both small companies and multinational corporations, trying to fix their computer systems so as to avoid an impending computer crises. Year 2000 remediation is not a modernization program; it is damage control. Each dollar spent remediating the problem is a dollar which might have gone towards modernization, production, infrastructure, expansion or some other use designed to improve government services or to build industry's better mouse trap. Instead, multitudinous man-hours and other limited resources are spent trying to do little more than insure that business and government will be able to continue doing on January 1, 2000 what they

---

[66] "Y2K ANNOUNCE: IQPC Houston Y2K Conf. Coverage," electronic mail received 22 June 1998 23:11:55 -0500 (CDT) from The Year 2000 Information Center, http://www.year2000.com. Kraft's experience is hardly unique. A BBC article reporting on the effects of the Year 2000 Problem in the United Kingdom noted that "[a]lready the first signs are appearing: Marks & Spencer came close to destroying a consignment of corned beef dated to expire in 2005, when their computer system read the date as 1905." Robin Guenier, Task Force 2000 and former Government Millennium advisor, as quoted online at http://www.bbc.co.uk/education/disaster/bug.shtml, site visited on October 21, 1998.

[67] "[Y]ear 2000-related glitches have already cropped up in many forward-looking computer applications, from drug-expiration dates to manufacturing systems. All provide a sneak preview of the problems expected to arrive in January 2000." Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[68] Electronic mail titled "Y2K Remediation Costs" from Heidi Hooper, <hhooper@itaa.org>, Director, Year 2000 Program, Information Technology Association of America (ITAA) (October 7, 1998) (on file with author).

[69] De Jager, Peter, *Moving to Zero*, September 1998, found at http://www.year2000.com/y2ktimeflies.html, site visited on October 21, 1998.

B. Curtis

were able to do on December 31, 1999. This remediation process has expanded the IT industry exponentially by creating enormously strong market forces for remediation products, analysts, surveyors, consultants, programmers and troubleshooters.

Beyond the actual dollar costs, the impacts of Y2K may be experienced from the remediation process itself . For example, Great Britain's National Pharmaceutical Association reported that "two pharmacies had their entire records wiped out whilst they were testing their PC system for Millennium compliance."[70] This is one of the difficulties posed where efforts to fix a computer system must be made while the system is operational. Many corporations and government agencies do not have the resources to allow remediation programmers to perform software repairs on a parallel system. In such cases, the programmers must survey the software, make the repairs and perform tests of those repairs while the system is operating, performing its normal functions. Under these conditions problems are bound to occur; when they do, the reality of the Year 2000 problem becomes abruptly apparent.

Furthermore, the Year 2000 problem has altered the way corporations do business, injecting a layer of secrecy between stockholders and corporate officers who are trying to avoid revealing the corporation's status with regard to the approaching date.[71] Businesses which are trying to determine how their relationships with suppliers and customers will affect them are encountering a wall of silence, erected--in part--by legal staffs attempting to limit liability. When companies send requests for information as to the Y2K compliance status of their suppliers, vendors, customers and anyone else with whom they deal electronically, the requests often go unanswered. Companies are left to conclude that even if they have remediated all of their own computer systems

---

[70] Robin Guenier, Task Force 2000 and former Government Millennium advisor, as quoted online at http://www.bbc.co.uk/education/disaster/bug.shtml, site visited on October 21, 1998.
[71] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998, *quoting* Noah Ross, vice president at Cap Gemini.

B. Curtis

before the turn of the century, their business interrelationships may keep them from operating productively.

The Year 2000 Problem will also be felt as industry prepares for the arrival of that fateful date. Companies that have adopted the "just-in-time" manufacturing practice for having parts, subcomponents and stock delivered to their manufacturing centers will (or at least should) be leery of whether their suppliers will still be able to meet delivery targets after January 1, 2000. Such skepticism may result in stockpiling or a flurry of changed business relations and partners as manufacturers look for vendors who are convincing when claiming they will be able to provide necessary materials on time. For those who fail to plan adequately, or whose faith in suppliers proves unjustified, delays, work stoppages, plant shut-downs, furloughs and layoffs may result. The same fate awaits those companies who have failed to properly address the Year 2000 problem in house. Their work forces will be involuntarily idled while trouble-shooting teams (once they are available) try to determine the cause for failures and make necessary repairs. Undeniably, the Year 2000 problem has already had an impact. The remaining question is how the second "shock wave" that rolls in with the next century will compare with the wave already experienced during these ongoing efforts.

2. *Seriousness of the Problem*

The problem is serious.[72] "The crisis is very real and potentially very costly."[73] Those words seem hardly worth quoting, considering how frequently the Year 2000 Problem is discussed in congressional hearings, industry meetings, and numerous seminars. Newspapers and other periodicals appear to be increasing their coverage on

---

[72] "The seriousness of this Year 2000 problem (or "Y2K" for short) is illustrated by the huge sums of money being spent to try to avoid it." Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998.

[73] Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998.

B. Curtis

Y2K, featuring more articles on the issue and chronicling government and industry efforts to avoid the fallout. The importance of the quotation rests less on its accuracy than its timing: it was made in an article titled "Doomsday 2000" published over 5 years ago in Computer World.

Claims of the problems that will result from the Year 2000 situation range wildly,[74] but frequently without any factual foundation from those who possess the requisite information to more accurately predict what problems will begin with the turn of the century. Unsupported extreme[75], and sometimes trite,[76] claims result partly from the sensational tendencies common among the media today, partly from media inattention to those speaking from educated positions on the subject, and mostly from the wall of silence erected by those whose agencies or corporations are not prepared for the millennial date change. There are, of course, more knowledgeable people speaking out on what we can expect in the Year 2000: "A disruption in the flow of information, especially if it is critically important information, might similarly disrupt global economic activity and produce a recession."[77]

---

[74] Which is probably why "TEOTWAWKI" (The End Of The World As We Know It) is becoming a popular acronym on the Internet. Joel Achenbach, *Y2K Fears Reach Beyond the Fringe*, WASH. POST, December 7, 1998, p A01, also available at http://www.washingtonpost.com/wp-srv/washtech/frompost/dec98/y2kfears7.htm, site visited on December 7, 1998.

[75] Claims that the United States will be subject to a nuclear missile attack or that planes will fall out of the sky following midnight, December 31, 1999, are "totally without foundation and have never been stated by any reputable computer consultant . . . ." De Jager, Peter, *It's a People Problem*, found at http://www.year2000.com/y2kpeople.html, site visited on June 22, 1998.

[76] The president sees that "the consequences of the millennium bug, if not addressed, could simply be a rash of annoyances, like being unable to use a credit card at the supermarket, or the video store losing track of the tape you have already returned," or "[i]t could affect electric power, phone service, air travel, major governmental service." Remarks by the President concerning the Year 2000 conversion, delivered July 14, 1998 at the National Academy of Sciences, and found at http://www.y2k.gov/new/presy2k.html (October 3, 1998).

[77] Armstrong Williams, *Millennium Bug's Painful Potential*, WASH. TIMES, August 29, 1998, at C1, *quoting* Dr. Edward Yardeni, "chief economist with Deutsche Morgan Grenfell and one who sounded the alarm early on, [predicting] that the millennium bug has the potential to wreak great havoc." *Id.* However, Jack Gribben, spokesman for the President's Council on Year 2000 Conversion, was quoted as saying "There's no evidence at this point to indicate that people should be disrupting their lives in any significant way because of the year 2000 problem." Joel Achenbach, *Y2K Fears Reach Beyond the Fringe*, Wash. Post, December 7, 1998, p A01, also available at http://www.washingtonpost.com/wp-srv/washtech/frompost/dec98/y2kfears7.htm, site visited on December 7, 1998.

B. Curtis

Initially there were those who doubted the seriousness of the Year 2000 Problem and the crises that were predicted, as though those voicing concern and warning were modern day "Chicken Littles," claiming that the cyber sky was falling. Early concerns about the problem may have been ignored under the assumption that the situation was too obvious and existed on so grand a scale that a technical fix had to be in the works. Considering how quickly software manufacturers update their products and seemingly force the obsolescence of earlier product versions, a more skeptical view may also have prevailed: the software services industry was overstating the problem to market their software repair services and to increase sales of their newest applications software or conversion software. However, as early as April 12, 1996, a Congressional Research Service memorandum noted that "[m]ost agencies and businesses . . . have come to believe that the problem is real, that it will cost billions of dollars to fix, and that it must be fixed by January 1, 2000, to avoid a flood of erroneous automatic transactions."[78]

With the increased amount of press and media attention being devoted to Year 2000 issues, more people are becoming aware of the Year 2000 problem and beginning to seriously consider what the ramifications might be for them personally. Predictions of what will befall our modern, technologically-driven world in the new century continue to range from the extremes of total breakdown accompanied by mass hysteria to something more akin to an electronic burp felt only by the truly cyber-minded.[79] Others hedge their bets, expressing predictions as a range of possible

---

[78] Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000 Computer Problem, Congressional Research Service, April 12, 1996, p. CRS-2. This same document suggested government and industry focus on repairing their most critical systems, considering that it was probably already too late to make necessary conversions to every affected system before the turn of the century.

[79] Testifying before the Government Reform and Oversight Subcommittee on Government Management, Information and Technology on June 22, 1998, Dennis Grabow, president of the Millennium Corporation stated that "[w]e're forecasting an economic recession, a global economic recession" as a result of one computer failure driving others to also fail. Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4.

B. Curtis

outcomes: "The best that can happen is that there will be failures and that unpleasant experiences will last for several months. The worst is that there will be a total breakdown of systems - a chaos in our world lasting for months or a year or more."[80] Somewhere in between--where the truth most often lies--are those who claim that some disruption is inevitable, but that as we continue to focus on correcting the problem before December 31, 1999, the disruption can be minimized both in scope and severity.

3. *Breadth of the Problem*

The amount of software to be converted to achieve Year 2000 compliance is enormous; executives in business and government should be keenly concerned with the problem and effectively spearheading remediation initiatives within their organizations. The Year 2000 problem will cause problems anywhere IT is used to calculate age, sort by date, compare dates, or initiate tasks based on date data. The two-digit year date format is well-nigh universal; it will be found in micro-code (within embedded processors), operating systems, software compilers, application programs, database queries, subroutines and procedures, data input screens and report formats, databases, and data files. Remediation efforts will have to address each of these areas to fully implement any Y2K solution. Nationwide annual computer services are estimated at about $150 billion.[81] Public sector remediation costs have been estimated between $50 billion[82] and $270 billion.[83] Therefore, the costs of converting non-compliant software into code which will work properly in 2000 will be somewhere between 30% and 180% of what is typically spent on IT in a year.[84]

---

[80] Robin Guenier, Task Force 2000 and former Government Millennium advisor, as quoted online at http://www.bbc.co.uk/education/disaster/bug.shtml, site visited on October 21, 1998.
[81] http://www.itaa.org/y2kga.htm, site visited on November 21, 1998.
[82] http://www.itaa.org/y2kga.htm, site visited on November 21, 1998.
[83] Remediation cost figures are discussed in greater depth in the section on Solution Issues. These figures are included here only to demonstrate the size of the Y2K problem relative to annual IT spending.
[84] http://www.itaa.org/y2kga.htm, site visited on November 21, 1998.

B. Curtis

The true scope of the Y2K problem is both hard to assess and indescribably large: hard to assess because it is impossible to accurately determine every program or processor that uses date information in performing its processing functions; indescribably large because software and microchip technology pervades practically every area of our technologically rich 20th century culture. The problem is unique in that it will be a world-wide event: January 1, 2000 arrives exactly the same day for every person in every country.[85] The Y2K problem will likely go down in history as the "shock wave felt round the world." Come the dawn of the new millennium, the world may observe a "first shall be last and the last shall be first"[86] technological day of reckoning where those nations which are most technologically advanced will be the most severely impacted by Y2K fallout and those nations which lag behind technologically will experience the least disruption of daily life.[87]

As an example, it may be that the Federal Government's attempts to streamline the acquisition process, moving to a totally electronic procurement system, will make the government more vulnerable to Y2K problems. The FAR directs Federal Government agencies to "use electronic commerce whenever practicable or cost-

---

[85] The actual dawn of that date will, as with every day, cascade across the globe's time zones one hour at a time, potentially allowing those at the end of the cascade process--just east of the International Date Line--to have a short-fused preview of the immediate results of this technological time-bomb.

[86] THE HOLY BIBLE, Matthew 19:30 and Mark 10:31 (reference the world-wide end-times described in the Bible where those who have become "last" by sacrificing earthly status and comforts to seek heavenly goals will become "first" in the eternal after-life existence, and vice versa).

[87] One writer records the conclusion of foreign analysis that "China, . . . is less vulnerable than many industrialized countries to the millennium bug due to a relatively low level of computerization." *China Sprays for Y2K Bugs*, Reuters Special to CNET News.com, October 21, 1998, found at http://www.news.com/News/Item/0,4,27792,00.html, site visited on October 27, 1998.

B. Curtis

effective."[88] Agency heads "shall ensure that systems, technologies, procedures, and processes used by the agency to conduct electronic commerce --

(1) Are implemented uniformly throughout the agency, to the maximum extent practicable;

(2) Are implemented only after considering the full or partial use of existing infrastructures, (e.g., the Federal Acquisition Computer Network (FACNET)) . . . ."[89] The Government's success at achieving its electronic commerce mandate is directly proportional to the risk it now faces due to the Y2K Problem, and makes the necessity of remediating Government systems all the more imperative.

If we were to mentally walk through a typical day, attempting to identify every Y2K-susceptible computing device that might touch our life, even with limited knowledge about computer-technology we would soon see the enormity of the problem looming before us with the turn of the century. Imagine the sunlight streaming through the window signaling that you have overslept. The digital display on the bedside clock is unlit. There is no fresh-brewed coffee smell wafting up the stairs, although the machine was set to begin brewing 15 minutes before the alarm clock was set to click on the local news station. And it is cold. Really cold. The electricity went out during the night and power must be affecting the gas-fired heater somehow too. The shower only spurts lukewarm water so you hurry through your shower. Your neighbor may not be so fortunate. By the time he showers, there may not be enough water pressure left in the municipal water system to push his tepid water through. Electricity and gas down; water off-line. Nothing left to do but get to work. Hope you plan to walk because one or more of the sixty or so microprocessors in your car are keeping it from starting. You

---

[88] FAR 4.502(a).
[89] FAR 4.502(b).

B. Curtis

could ride a bike to work; there are no cabs, buses, trains or subways working--they are just as off-line as your car. When you try to call the office to say you cannot make it in today, the phone apparently has power but there is no dial tone, just a high-pitched metallic sound as though you were connected to a facsimile line. Fortunately your apartment is on the first floor. Those higher up will be getting aerobic exercise on the stairs until the microprocessors in the elevator's control system are replaced. The story could go on and on--and it may, depending upon how accurate predictions are and how successful we are with efforts to change this future through remediation.[90]

There is no distinction between government and commercial IT systems where the Year 2000 Problem is concerned: computing equipment will be affected, regardless of who it belongs to and what it is being used for. For that matter, organized crime's computers will suffer the same fate as the Justice Department's, assuming neither is made Y2K compliant before 2000. The Global Positioning System (GPS) is used world-wide by military and commercial airlines, naval fleets, luxury automobiles, and consumers for a wide variety of applications to precisely determine one's location anywhere on the face of the globe. This system is not yet Y2K compliant.[91] Most of the software changes which must be made to computer systems on-board the satellites that make up the GPS "constellation" can be uplinked to the satellites from control and

---

[90] Some people are following the Boy Scout admonition to 'be prepared" as they make preparations for the disruptions they expect to arrive with the Year 2000. Wood fireplaces or wood, pellet or kerosene stoves may provide needed warmth if conventional power utilities fail. Refrigerator power and food-supply lines may be down long enough that some people are stocking up on nonperishables, such as tuna fish or other canned meats; dried beans, rice, pasta, egg protein powder, cheese food. Water—treated with one drop of clorox per gallon—and paper products are practical necessities. Some have purchased manuals on hunting and survival techniques and others are planning to have a firearm for safety and protection. Such preparations may sound to some like an overreaction, typical only of "survivalist" types or militia members, but people from the mainline who have become familiar with what Y2K may bring are beginning to make these types of plans for the coming date. Joel Achenbach, *Y2K Fears Reach Beyond the Fringe*, WASH. POST, December 7, 1998, p A01, also available at http://www.washingtonpost.com/wp-srv/washtech/frompost/dec98/y2kfears7.htm, site visited on December 7, 1998.
[91] Interview with Mark DallaBetta, formerly the Y2K Project Officer for U.S. Space Command and North American Aerospace Defense Command, currently the Deputy Director of the Marine Corps' Computer and Intelligence Activity, a division of C4I, Headquarters Marine Corps. The GPS information was provided as of June 1998.

B. Curtis

monitoring stations on the earth's surface. The more difficult issue involves the embedded processors which will need to be manually reprogrammed, if possible, or replaced. Fortunately, the processors that require reprogramming are located in the ground control stations rather than on-board the satellites.

Both legacy systems and personal computers (PCs) require Y2K remediation. "Legacy systems" are those systems which have been the computing workhorses for past decades and even now continue to carry the bulk of the workload for many government agencies and segments of corporate America. Because these systems are, by definition, older than most, there is more likelihood that they will not be Year 2000 compliant. Adding to the bad news, the programming language of these systems, often COBOL, are not frequently used by today's programmers; therefore, the first step in remediation may entail bringing software programmers out of retirement. Some PCs may already be Y2K compliant, depending upon when and by whom they were manufactured; however, some have predicted that "[s]ystem clocks on virtually every personal computer will wind up with corrupted dates on January 1, 2000."[92] Considering the relatively quick turnover of PCs and their peripherals in many organizations, it may be possible to schedule Y2K-compliant acquisitions into the normal replacement planning.

In addition to the typical legacy computer system and the desktop PC, "[l]ocal area network and interface devices, [and] telecommunications systems . . . are also susceptible and unless fixed in a timely manner may also fail to properly operate when faced with dates after December 31, 1999."[93] "The big risk to all infrastructure is the risk of cascade failure--the risk of one person taking down everybody else . . . ."[94] Clearly

---

[92] *The Year 2000 Problem*, found at http://www.itl.nist.gov/div897/info2000.htm, site visited on November 21, 1998.

[93] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[94] Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4, *quoting* Dan Steinberg. Steinberg, president of the Canadian firm Synthesis: Law and Technology,

the Year 2000 Problem knows no boundaries between government and the private sector; both are equally susceptible individually and through the connectivity that has come to characterize both interagency relationships as well as business relationships at the end of the twentieth century. January 1, 2000 arrives the same day for everyone around the globe.[95] nearly simultaneously

Telecommunications is probably the best example of an almost totally computer-dependent industry whose computer reliance is invisible to the majority of Americans and which is integral to business and government, and touches many aspects of most peoples' life. The computer-supported functions provided through telecommunications networks are transparent to the typical service customer, whether that person is making a simple local or long-distance phone call on a corded, cordless, or wireless phone; writing a check on funds which were electronically transferred to his account with a financial institution; waiting for police to arrive after an intruder alert system sounds an alarm at a remote monitored facility; depending upon emergency broadcast and response networks to warn of deadly weather or foreign military attack; viewing or listening to broadcasted programs via radio, television, or Internet terminal; sending data to a remote location via facsimile, electronic mail, or other video communication media; receiving health care in a private physician's office or a regional medical center; using gas and electric power for heating, cooling and powering appliances; and counting on national security systems to provide adequate defensive and necessary offensive capabilities to protect the nation.

---

was testifying in the June 22, 1998 hearings before the Government Reform and Oversight Subcommittee on Government Management, Information and Technology.
[95] With the earth's rotation and our staggering of "time" along time zones across the world, the Y2K deadline will actually arrive in 24 separate increments, starting with the International Date Line, rather than simultaneously.

B. Curtis

4. *Resulting Problems*

a. Problems Already Experienced

As mentioned above, corporations are remaining rather tight-lipped when the Year 2000 is the topic.[96] They are reluctant to share their current compliance status, their projections for the degree of compliance they expect to achieve, the timelines they have drawn for reaching that status, and any Year 2000 failures they have already experienced. While the risk of future litigation is a key reason for such secrecy, many companies are maintaining silence so that their customers and investors will not lose confidence in the company.[97] One writer concluded that "its not only lawyers who sense this potential flood of litigation, the financial community has reported similar liability based concerns as potential investment risks."[98] It remains to be seen whether the newly enacted federal statute, The Year 2000 Information and Readiness Disclosure

---

[96] The federal government is not necessarily being any more candid that corporations regarding Y2K preparedness, and possibly for some similar reasons. Government officials certainly are not eager to bring criticism on themselves, their management effectiveness, or the agencies they serve. Additionally, officials want to avoid creating a sense of public panic--particular in banking where "runs on the bank" can have devastating effects on the economy. The FDIC has conducted readiness tests to gauge the Y2K preparedness of individual banks; however, the performance results have not been made available to the public. YEAR 2000 ASSESSMENT RATING, FINANCIAL INSTITUTION LETTERS (FIL-74-98), Federal Deposit Insurance Corporation, July 8, 1998.

[97] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998, *quoting* Noah Ross, vice president at Cap Gemini.

[98] DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998), at 580-81, *citing* B. AUSTRIAN & T. PAGEL, MILLENNIUM MORASS (Montgomery Securities 1997), at 45. Corporate concerns, both of litigation and investor confidence, are well-founded. Acquisitions and mergers may also be affected by the Y2K issue. Before acquiring another business entity, a corporation would be foolish if it did not assess the potential cost to make the target enterprise Y2K compliant. Perhaps mergers and acquisitions can be made contingent upon compliance costs being within a dollar figure and completion date cap. Even with an escape clause, difficulty will still arise if the acquired interest does not meet the deadline or the compliance costs exceed the established caps: marriages made on Wall Street are not often inexpensive to annul. For a discussion of critical areas for management inquiry when acquiring a business interest with potential Y2K compliance issues, see DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998), at 580-81.

B. Curtis

Act,[99] will calm corporate fears and lead to the type of information sharing so desperately needed to reduce the learning curve and speed the remediation process throughout industry and even government.

Some federal agencies have already had a taste of the interruptions and delays that draw closer each day with the coming of the Year 2000. In 1997, the Defense Logistics Agency, which supplies food, clothing, medicine and fuel to all Department of Defense agencies, experienced a date calculation error in its computerized materiel management system.[100] The system erroneously dropped 90,000 items from DLA's inventory, and required approximately 400 man-hours to correct the problem.[101]

State computing systems have also had a sneak preview of the millennium's coming attractions:

> When Mary Bandar didn't report to kindergarten as instructed by Minnesota state officials in 1993, she had a valid excuse: The 104-year-old Winona resident had already done her time with blocks and crayons. State computers mistook her as a 4-year-old because "89" was at the end of her birth date.[102]

This case highlights the fact that the computer problem is not truly a "Year 2000" problem or even a "millennium bug." Rather, it is merely the computer's inability to produce accurate data or results when its assumption that all dates encountered are dates from the 1900s. Dates from the 1800s, such as Mary Bandar's date of birth, will produce just as erroneous a result in a computer system which performs its processes on only the last two digits of a year as will dates from the Year 2000 and beyond.

---

[99] Year 2000 Information and Readiness Disclosure Act, 1998, Pub. L. No. 105-271, 15 U.S.C. δ1 (Note) (1998), *reprinted in* ELECTRONIC COMMERCE & LAW REPORT (BNA) Vol. 3, No. 42, at 1283 (November 4, 1998). The statute is discussed below in the chapter on legislative, executive, and agency options.
[100] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.
[101] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.
[102] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

B. Curtis

The public financial service industry was one of the first to be hit with Year 2000 failures, largely due to its heavy reliance on computer technology. Financial systems perform numerous date calculations and contain forward-looking applications, used to forecast rates and payments and provide statistical information for investment strategies. "[T]he financial service industry was hit by the first wave of year 2000 snafus. Until recently, retail point-of-sale systems couldn't read credit cards with '00' expiration dates."[103] Consumer complaints regarding faulty card-readers prompted Visa International to ban its member banks from issuing credit cards with expiration dates of 2000 or beyond. Only after most of the card-readers had been adjusted or replaced in October of 1998 did Visa lift the ban. [104] In fact, the first Year 2000 lawsuit filed stems from the inability of computerized cash registers to read, or at least honor, credit cards with expiration dates beyond 1999.[105]

Manufacturing in the commercial sector has likewise been given a glimpse of what lies ahead by early computer-driven foul-ups. The $6 billion a year Amway Corporation, based in Ada, Michigan, has had two bites from the millennium bug.[106] The first was detected in mid-1996 in one of the corporation's mainframe computers. One of the applications on this mainframe was a five-year forecasting system. It was determined that the five-year system was only forecasting out three years and eight

---

[103] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[104] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[105] *See* Produce Palace v. TEC-America Corp., *et al.*, No 97-330-CK, Mich. Cir. Ct., Macomb, Co. The plaintiff has asserted claims for breach of warranty, violation of the Magnusson-Moss Warranty Act, breach of warranty of fitness, revocation, breach of duty of good faith, misrepresentation, breach of contract, and violation of the Michigan Consumer Protection Act, seeking damages in the amount of $10,000 plus legal fees. *ITAA's Year 2000 Program, Year 2000 Law Suits (Filed & "Potential")*, found at http://www.itaa.org/Y2Klaw.htm#Federal, site visited on September 4, 1998. *See also* Linda A. Monica, *Year 2000 the Gathering Storm of Litigation of the "Millennium Bug,"* 13 ME. B.J. 184 (1998) for a discussion of this and several other cases under the topic of "Vendor Liability."

[106] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

B. Curtis

months--the amount of time remaining before the Year 2000. The system had truncated the forecast, unable to project beyond the date boundaries it understood. The second came late in 1997 when a mixing system in one of their manufacturing centers rejected a batch of chemicals used in making one of the Amway cleaning products. It seems the mixing system, which was driven by a PC (personal computer),[107] viewed the chemicals as unusable, interpreting the "2000" expiration date on the chemicals as "1900."[108]

One positive outcome from early glitches is the reality check those snafus provide for some corporate officers and the increased attention towards remediation efforts that tends to result after a company experiences a date-related error or system failure.[109] Amway's Year 2000 coordinator stated that Amway's "senior management's attitude was that 2000 was a long ways off, and we'll fix it later," but that after the failures occurred, "they figured they better look more closely" at Y2K issues now.[110] An analyst with the Gartner Group phrased it this way: "For most companies, all it takes is

---

[107] PCs (or personal computers) typically refer to one of a series of microcomputers produced for small, stand-alone computing applications, such as those used in many households. Apple and IBM-compatible products, such as the Intel 286, 386, 486 and Pentium processors, fall into the category labeled "PCs" and are sometimes used to drive equipment or process controllers in industrial applications. Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998). Mr. Kellett is an attorney with GSA and has a technology background which includes engineering applications for industrial manufacturing systems.

[108] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[109] While checking the computer systems at its Rhode Island Hospital Trust affiliate, BankBoston detected date problems which could have erroneously recognized customer certificate of deposit accounts as 100 years old and transferred them to a lost-and-found bin for transfer to the state under statutory provisions governing stale accounts. Steven McManus, communications manager for BankBoston's Millennium Project Team stated that the early (1996) detection "was a real eye-opener" and helped his team "break through some of the denial" of the problem they had encountered among some of the corporate management. Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[110] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

B. Curtis

one good failure, and they get religion right away."[111]   Furthermore, early detection--
even if in the form of a processing malfunction--allows an agency or company to isolate
and solve problems before what will likely be a mad-dash on a grand scale in January
2000.

b. Potential or Anticipated Problems

If not corrected in time, the Year 2000 Problem could spawn an array of
problems almost too vast to contemplate, affecting the obvious--computers and
computer-related products and systems--and numerous other areas of our daily
environment that we do not associate as being related to computers.   The World
Information Technology and Services Alliance claims that

> incorrect date processing will mean businesses will be unable to process orders,
> dispatch invoices, calculate payments, process transactions and so on.
> Government may not be able to issue checks, calculate tax returns, or produce
> forward-looking budgets. In addition, computers are built into different types of
> equipment such as elevators, automobiles, and appliances which have date
> processing functions, and which may become inoperable with unpredictable
> results. The problem is so pervasive that it has the potential to severely disrupt
> not only individual businesses, but whole economies.   This is compounded by
> the fact that almost all computer-based systems worldwide are affected with this
> problem at the same time.   And the date by which solutions must be found is
> immutable.[112]

One need not look beyond the federal government to consider the negative
impact that could result from the Y2K problem, particularly if left unaddressed or not
properly remediated in a timely fashion.   In his testimony before congress, Arthur
Gross, former IRS Associate Commissioner for Modernization, explained the
seriousness of the situation posed by Y2K at the federal tax agency: "[F]ailure to

---

[111] Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998, found at http://www.idg.co.nz/nzweb/aaea.html, site visited on October 20, 1998.

[112] WORLD INFORMATION TECHNOLOGY AND SERVICES ALLIANCE (WITSA) WHITE PAPER, *The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and Governments,* found at http://www.itaa.org/witsay2k.htm, site visited October 21, 1998. WITSA, is an organization composed of representatives from twenty-eight different information technology industry organizations from around the world. WITSA serves a public policy roll, and "believes that governments and international organizations worldwide must immediately address the very serious threat posed to both individual nations and the global economy by computer processing problems resulting from the advent of the Year 2000." *Id.*

identify, recode and retest each . . . date-based [field in IRS records] . . . could result in the generation of millions of erroneous tax notices, refunds, bills, interest calculations, taxpayer account adjustments, accounting transactions and financial reporting errors."[113] The General Accounting Office smothered hopes that these predictions would all be avoided through remediation, noting that "the IRS is one of the agencies least prepared to deal with the year 2000 problem."[114] Senator Robert Bennett cautions that the Y2K problem could cause delays in the government's ability to make Medicare and Medicaid payments. As a result, "[t]here are health care entities that may very well go bankrupt because they cannot get reimbursement from Medicare and Medicaid."[115]

If the Y2K problems in government IT systems are not corrected before January 1, 2000, the Social Security Administration's computers may perform calculations which conclude that 25-year-olds are 75-years olds.[116] If the SSA miscalculates citizens' ages, the government will likely end up paying benefits to those who are not truly eligible for them while at the same time cutting off benefits to those who are actually entitled to them.[117] The IRS could miscalculate the standard deduction on income tax returns of those persons over age 65, causing inaccuracies in the agency's records of revenues received and amounts due.[118] DoD weapons systems which use date data could either fail altogether, leaving us without a defensive capability, or--worse yet--malfunction and

---

[113] Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998, *citing* Arthur Gross, IRS Associate Commissioner for Modernization (since resigned), congressional testimony quoted in *IRS Countdown to Meltdown*, INSIGHT, November 3, 1997.

[114] Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998, *citing* Clausing, The New York Times, May 8, 1998.

[115] Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998, *citing* Bennett, July 15, 1998.

[116] *See* Statement of Representative Peter Blute before a hearing of the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight, "Is January 1, 2000 the Date for a Potential Computer Disaster?" April 16, 1996.

[117] Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000 Computer Problem, Congressional Research Service, June 7, 1996.

[118] Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000 Computer Problem, Congressional Research Service, June 7, 1996.

B. Curtis

possibly have something more terrible occur.[119] Official computer systems at all levels of government could malfunction, causing records corruption and resulting errors in every kind of governmental computing system. Malfunctions could affect income, sales and property tax records; payroll and retirement systems; utilities regulations and public transportation; and motor vehicle licensing, titling and registration. - [120]

The Senate Committee on the Year 2000 Technology Problem, chaired by Senator Robert Bennett has been conducting hearings which focus on different industries, asking witnesses to describe the risks posed by Y2K problems in their industry, the efforts being made to head off those problems, and the status of those efforts. The first of these hearings, held June 12, 1998 was titled "Hearing to Discuss Chances the Millennium Bug Will Cause the Nation's Power Grid to Fail." At that hearing, Senator Bennett stated that if January 1, 2000 were to have come that weekend, the answer to the hearing's question would be 100%, but that because the power industry had 18 months left to address Y2K concerns, the chances were more like 40%.[121]

The interest in the Y2K status of power utilities is long overdue and may have come too late to avert real problems. One press account announced: "Many electric utilities realized only last year that their generating plants were susceptible to Y2K problems. Scattered power outages are likely, and some nuclear power plants may shut down temporarily."[122] The Electric Power Research Institute conducted a workshop for executives from utility companies. In summarizing the event, the host concluded,

---

[119] See generally Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000 Computer Problem, Congressional Research Service, June 7, 1996.
[120] See generally Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000 Computer Problem, Congressional Research Service, June 7, 1996. Representative Blute noted that date calculations could result in driver's licenses expiring prematurely. Statement of Representative Peter Blute before a hearing of the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight, "Is January 1, 2000 the Date for a Potential Computer Disaster?" April 16, 1996.
[121] June 9, 1998 press release, found at http://www.senate.gov/~bennett/pr609b98.html, site visited on September 3, 1998.
[122] Where the Bug Will Bite, BUSINESS WEEK, Mar. 2, 1998.

B. Curtis

"Despite the industry's best attempts, there will probably still be some problems that will not be resolved, necessitating some degree of emergency/disaster planning."[123]

One industry expert[124] has refuted the assertion--he calls it one of the Y2K myths--that if one of the four regional power grids fails ("goes black"), operators will not be able to restart it right away. He explains that many power plants have backup diesel generators for restarting the power plant and that once any plant within a grid has restarted, it can produce and transfer adequate power to the other plants in the grid to allow them to restart, if they were not able to do so via their own backup methods. He points to the blackouts of the last decade and claims the industry has learned lessons from those events.[125] What this expert's comments fail to address is how the computer-driven system controller that took a grid off-line will be quickly found and fixed so that the emergency response procedures he describes will successfully bring the grid back up. If the condition that caused the failure is not remedied, it would seem that restarting the grid--assuming that is possible--will do nothing but begin a cycle of restarting and refailing.

At the June 1998 hearings before the Information Technology subcommittee, an invitee made a sobering suggestion: "The question 'How will a launch system react if it believes it has lost communication with its command and control masters for 100 years?' should be asked of world leaders."[126] With all of the ill results that are being discussed, proclaimed and debated, the truth is that we just do not know the full extent

---

[123] David Lore, *Will New Century Shut Off Utilities?*, COLUMBUS DISPATCH, January 12, 1998.

[124] For over 20 years, Dick Mills (dmills@albany.net) has created the software used in power plants and power systems. In 1997 Mills traded his career to work exclusively on the Y2K issues surrounding power grids. http://www.y2ktimebomb.com/Bios/dmbio.htm, site visited on October 21, 1998.

[125] Dick Mills, *Another Myth, A Black Grid Can't Be Restarted*, August 14, 1998, found at http://www.y2ktimebomb.com/PP/RC/dm9832.htm, site visited on October 21, 1998.

[126] Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4, *quoting* Alan Simpson. Simpson, president of ComLinks.Com, testified at the June 22, 1998 hearings before the Government Reform and Oversight Subcommittee on Government Management, Information and Technology. Simpson blamed the president for not doing enough to head off the Y2K problem, stating that "In the new global information age, we would have assumed that the leader of the United States would have led the global awareness and rectification campaign. We assumed wrong." *Id.*

of what awaits us. Alan Greenspan put it this way while addressing the Senate Banking Committee: "We do not know or cannot realistically make an evaluation of what the economic impact is as a consequence of the [computer] breakdowns that may occur. We do not know the size. We do not know the contagion and interaction within the system. And we do not know how rapidly we can resolve the problem.[127]

D. TECHNICAL SOLUTIONS

Year 2000 remediation has already become a booming business. Software manufacturers are scrambling to market Y2K software repair tools and database conversion programs, and IT service companies are profiting in a market whose supply is far smaller than the demand. The Internet has become one of the most popular means of advertising remediation products and services, with vendors slipping their product announcements into the Y2K information mailings and postings in exchange for underwriting the costs of those Internet services.[128] Whether an organization attacks the Y2K problem with in-house resources or enlists the aid of commercial remediation tools or even a remediation contractor, the technical solutions available are the same.

1. *Four-Digit Year Date Fields*

The most obvious solution, and perhaps the one least likely to pose any negative side effects or operating limitations, is the four-digit year date field. Adding two digits to the year portion of a date field, so that dates previously processed and stored as "98" would now be "1998," sounds rather uncomplicated, but time, money, effort, and sometimes difficulty of making this conversion should not be underestimated. Software tools are available to assist in making these changes everywhere a year field exists, whether used in an application or stored in a data file. Still, these automated tools

---

[127] Testimony of Alan Greenspan, Chairman, Federal Reserve, before the Senate Banking Committee (February 25, 1998).
[128] The Year2000.com Stocks Page, claiming to "provide[] a comprehensive and up-to-date listing of public companies that represent that they provide Year 2000-related products or services," is found at http://www.year2000.com/y2kstock.html, site visited on November 11, 1998.

B. Curtis

cannot always detect when a date is being used in a calculation or some other process, so errors can be expected, whether automated tools or manual approaches are used. All that is to say, whatever solution is chosen, and whatever method is used to implement that solution, verification testing will be necessary to produce any meaningful level of confidence in the conversion effort.

A date format using four digits for the year complies with both the American National Standards Institute (ANSI) and International Organization for Standardization (ISO) standards for date formats. The ANSI standard for date format, ANSI X3.30, called for eight-digit date fields (DDMMYYYY)[129] The ISO standard for date format, ISO 8601, International Standard for Date and Time, also uses an eight-digit date field, but arranged just the opposite of the ANSI format: YYYYMMDD.[130] The ANSI and ISO standards for date format both use eight-digits, but the formatting schemes are totally incompatible. Applications programmed to accept date data in the ANSI format will have just as serious a problem receiving data in the ISO format as they would receiving the older, non-compliant six-digit date data. Clearly it is important to have consistency in the date format selected.

The Federal Government adopted the ANSI X3.30 standard as Federal Information Processing Standard (FIPS) 4-1, but because each element of the standard is optional, government computing resources frequently programmed with two-digit year formats for the same reasons as the rest of the software programming community. The

---

[129] *Millennium Rollover: The Year 2000 Problem*, found at http://www.itl.nist.gov/div897/yr2000.htm, site visited on November 23, 1998. In this format DD indicates the two-digit day and MM the two-digit month (including a leading zero for numbers less than ten), and YYYY indicates four-digit year. In recognition of the fact that this standard was applied to numerous applications for varied purposes, each component of the format was optional, so that the two-digit year date formats so widely used in software programming were in compliance with the ANSI standard. *Id.*

[130] *See* Ian Galpin, *Year 2000 and ISO 8601 Notes,* last revised February 2, 1998, found at http://www.aegis1.demon.co.uk/y2k/y2kgen.htm, site visited on November 21, 1998. The ISO standard is sometimes expressed in variant form, such as displaying March 24, 1987 as "1987-Mar-24" rather than "19870324" in an attempt to be more user-friendly to those who are not accustomed to this format. The format is familiar to the scientific community, particularly the field of Astronomy, where date data exchanges often cross international boundaries. Additionally, multi-national corporations have begun converting to this format as they attempt to avoid Year 2000 software problems. *Id.*

B. Curtis

National Institute of Standards and Technology (NIST), a Division of the Commerce Department, issued a March 25, 1996 Change Notice to FIPS 4-1 to ease the process for federal agencies planning their Year 2000 transitions.[131] The change stated that

> For purposes of electronic data interchange in any recorded form among U.S. Government agencies, NIST highly recommends that four-digit year elements be used. The year should encompass a two-digit century that precedes, and is contiguous with, a two-digit year-of-century (e.g., 1999, 2000, etc.). In addition, optional two-digit year time elements specified in ANSI X3.30-1985(R1991) should not be used for the purposes of any data interchange among U.S. Government agencies.[132]

In 1991, the DoD adopted several standards for storing date data, each of which requires the year to be represented by four-digits. Under these standards, dates can be expressed as "YYYYMMDD" (like the ANSI standard with no options taken) or "YYYNNN" (the year plus the three-digit ordinal date from 1 to 366) or "YYYY" (if only the year is required).[133] DoD Directive 8320.1 requires the use of this standard in all DoD applications and systems built since the 1991 adoption of the standard, including those that have been changed substantially, meaning that at least 30% of the code has been modified.[134] The DoD Year 2000 Management Plan provides guidance while still allowing some flexibility, instructing that

> DoD Components should use four digits (YYYY) for the year portion of dates used for interfaces among systems and in all interagency information exchanges unless the risk to do so, in terms of dollars, schedule, and technical issues, would be too high. The 4-digit date format is recommended, not required, for

---

[131] *Millennium Rollover: The Year 2000 Problem*, found at http://www.itl.nist.gov/div897/yr2000.htm, site visited on November 23, 1998.

[132] *Millennium Rollover: The Year 2000 Problem*, found at http://www.itl.nist.gov/div897/yr2000.htm, site visited on November 23, 1998. NIST recognized that the "optional elements" provision in the ANSI date format standard allows programmers and data exchangers to use non-compatible formats when attempting to exchange date data electronically.

[133] DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998, at Appendix J: DoD Standard Date Formats, found at http://www.dtic.mil/c3i/y2k/AppJ.html, site visited on October 27, 1998.

[134] DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998, at Appendix J: DoD Standard Date Formats, found at http://www.dtic.mil/c3i/y2k/AppJ.html, site visited on October 27, 1998.

B. Curtis

system interfaces and data exchanges in DoD to reduce the risk of re-infection of Y2K problems in the Department's systems and databases.

In Electronic Commerce (EC)/Electronic Data Interchange (EDI) transactions, where other formats are used, the Components should use 4-digit dates unless an agreed upon alternate has been established. Those systems using an ordinal date format must use the proper format (YYYYNNN). If a system is Y2K compliant but does not use a standard date format, conversion to the standard is not required.[135]

This guidance focuses on data interfaces and demonstrates that the DoD is moving to the type of data exchange standard that will be required in the Year 2000. It also makes it clear that agencies need not perform additional software or hardware conversion merely to meet this requirement if their computer technology is already Y2K compliant.

2. *Windowing*

Windowing attempts to solve the two-digit year problem by providing an algorithm for the system to use when processing date data. The computer may be instructed to treat two-digit dates from "10" to "99" as dates from the 1900s and two-digit dates from "00" to "09" as dates from the 2000s.[136] The computer will use the algorithm to examine two-digit year dates and make the appropriate conversion before performing operations on the date data. For instance, a computer with this windowing algorithm would convert the digits "00" and "18" to the dates "2000" and "1918" before subtracting (2000 - 1918) and would determine that the individual was 82 years old and, therefore, should not be mailed a notice to register with the government for potential conscription into the armed forces.[137] This technical solution is a more likely candidate

---

[135] DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998, at Appendix J: DoD Standard Date Formats, found at http://www.dtic.mil/c3i/y2k/AppJ.html, site visited on October 27, 1998.

[136] As an example, Microsoft's SQL Server uses windowing to address the century change, splitting the century in half. Two-digit dates are automatically adjusted to four-digits upon entry, with years greater than 50 assigned a "19" prefix and years up to 50 assigned a "20" prefix. *See* Timothy Dyck, *Y2K-Proofing Your Databases*, PC WEEK, October 19, 1998, found at http://www.zdnet.com/pcweek/stories/news/0,4153,360733,00.htm, site visited on October 27, 1998.

[137] Without this algorithm or some other Y2K solution, the system could subtract 18 from 00 and get 18 (as many systems have no mechanism for dealing with the unexpected/impossible negative subtraction

B. Curtis

for selection in applications that have relatively few date processing routines or functions that are used repetitively on a large scale basis.[138] There will not be a large number of software modifications to make, and any massive data files need not be changed at all. Assuming the organization desires to eventually shift to a four-digit date standard, that change may be made when the applications are migrated to new IT.

This solution is not without disadvantages. The first is the difficulty in determining the appropriate algorithm. Is the data handled discreet enough that two centuries will be sufficient, or will dates from additional centuries (beyond just 1900s and 2000s) be processed? More importantly, where should the break in years occur? "00" to "09" and "10" to "99" would work, at least for a decade, for the registration application described above, but it would not work for a mortgage lender's amortization program or an insurer's life-expectancy risk computations. That means one solution will not fit all applications. Even in a single application, the dates processed may be too diverse to allow for any windowing algorithm that will work for all data provided. The assumption that "33" is "1933" might work in one situation but not another, where "2033" is actually intended.

Secondly, whatever algorithm is selected, that "window" will only be valid for a certain period of time. Eventually time will progress and the window will not fit the data being processed. In the compulsory registration example above, the Year 2010 will arrive, and the system will treat the current date as 1910, perform the calculations accordingly, and notices will be generated for persons born between 1928 and 1999. One solution to this problem is to create a "sliding window" or "moving window" which may be adjusted, possibly shifting the window one year on an annual basis along with the actual passage of time, or less frequently as the window period approaches a boundary. In commenting on the interim FAR Y2K compliance provisions, the Chair of

result). Some unsuspecting octogenarian might be rather startled to learn that "Uncle Sam" still might need him in case of war.

[138] It would also be a less expensive solution where two-digit date chips could not be readily replaced.

B. Curtis

the Government Contracts Section of the Federal Bar Association noted that requiring a technical solution which will work for the entire twenty-first century eliminates windowing as a potential solution.[139]

For some organizations, the greatest disadvantage will be the inability of a system to properly interface with another system using a different algorithm. This problem may be minimized by ensuring the algorithm changes dates only within the internal processing routines and functions of the application software. Wherever the program provides or receives date data, the original two-digit year format will be used. The interfacing systems will then perform whatever algorithm it uses to ensure accurate date processing, and there will be no improper date exchanges as the systems interoperate. Where this solution is not feasible, it may be possible to write an interface program that specifically addresses the differences between the algorithms used by the two systems and automatically converts the data as it is exchanged.

As long as these drawbacks can be adequately addressed, the windowing solution will provide a cost-effective means of addressing Y2K compliance for a particular segment of IT users.

3. *Encapsulation*

Encapsulation is another algorithm-based approach that essentially avoids the Year 2000 problem in date processing by ensuring the internal software never encounters a date beyond 1999. The algorithm consists of an offset, a certain number that will be subtracted from incoming dates and then added to the resulting outgoing date after the processing is finished. The most-commonly used offset is 28 because the Year 1972 (2000 - 1972 = 28) was the last year when the days of the month and week were aligned as they will be in 2000. As a greatly-simplified example, suppose the application process is supposed to add ten years to the number provided to the

---

[139] Comments from Alex D. Tomaszczuk, Chair, Government Contracts Section, Federal Bar Association, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat).

B. Curtis

program. If the date "2006" is input to the system, the date "2016" should be returned. First the conversion algorithm would reduce the input date "2006" by the offset (2006 - 28) to produce the internal date 1978. The internal process would add ten to the date (1978 + 10) and return the resultant date 1988 to the conversion algorithm. The offset would be added back to the internal date (1988 + 28) and the date "2116" would be output as designed. This method could easily be coded to function properly whether dates were input in four-digit or two-digit year formats.

There are several drawbacks to this solution. First, picking the "right" offset presents a problem. The offset must be large enough so that when it is subtracted from the input date, the internal date is something earlier than 2000. At the same time, the offset cannot be so large that it will convert an input date into something earlier than 1900. The encapsulation algorithm could be made a bit more complex, dynamically determining a distinct and appropriate offset for each individual input date based on the particular application process, but in order to keep dates, months and days accurately lined up it would be best if the offset were a multiple of 28. Some application processes simply may not permit this solution because interim calculations during the internal processing would produce results greater than 99 or less than 0, regardless of the offset used.

Another drawback is that some applications are keyed to specific years coded directly into the software, and because the encapsulation process does not allow the internal processing to address actual dates, erroneous results could be produced. Suppose the process attempts to normalize sales performance by averaging an employees sales volume for each year. The program may have a feature which takes annual inflation into account based on the national figures for each year. The program may also correct for years in which sales policies were different so that one years sales (for instance 1991) are counted double and those in other years are accorded the face value. Based upon the offset date, the computer would produce improper information

B. Curtis

due to the fact that it was not applying the computational rules during the correct years. Sometimes a computer can only do its job correctly if it really knows the date.

Lastly, as with windowing, an offset for encapsulating date data has a "shelf life" no greater than itself. An offset of 28 from the current date of 2028 will produce an internal date that will not work in the application. This solution will demand algorithm modification at some point in the future, to be determined by the offset selected.

4. *System Clock Setback*

This solution is not unlike encapsulation except that it is aimed at systems which do not exchange date data with external sources. Rather, these devices only use date data, or more typically *time* data, for internal processing. These systems do not really need to know what the actual date is; they need to determine time relatively so as to accurately complete time functions and procedures. With such systems the easiest solution may be to "trick" the computer by setting back the internal clock. Setting the system back exactly 28 years will allow proper line-up of days of the week and month to current dates. Personal computers which are not interfaced with other equipment may be well-suited to this "work around" solution. Additionally, some process controllers with no connection to outside date information may be kept functioning beyond 2000 with this fix. However, great care should be used in determining that the system need only use relative time rather than actual time data.

5. *Replacement*

If an organization solves its Y2K problem by replacing its non-compliant systems, rather than attempting to remediate existing IT, the compliant equipment it acquires will have used one of the other technical solutions listed in this chapter. Some manufacturers have simply modified old, existing software with a technique such as windowing for the same reasons an organization may select that solution over another. Newly developed products will likely have used the 4-digit year solution as that

B. Curtis

resolution poses the least drawbacks and conforms to what is becoming the world-wide date format standard.

Some organizations have been struggling with old legacy computer systems for years, pouring maintenance dollars into upgrades, "patches," emergency fixes, and costly maintenance service contracts. In these situations, system renovation may not be a cost-effective solution. In some cases, Y2K remediation may not even be possible. Replacement purchases may be the only option available to some agencies for achieving Year 2000 compliance.

Amongst the nation's ten largest utility companies, the typical company anticipates it will replace or retire 25% of its non-compliant systems and renovate the other 75%.[140] In addition to the remediation efforts currently underway, the DoD plans to replace 203 of its 3,143 mission critical systems.[141] Y2K remedies are as diverse as the organizations they serve. Some organizations would do well to replace the majority, if not all, of their systems. This would be particularly true where an agency's long-term IT procurement plan already called for modernization of aging equipment due to constraints beyond the Year 2000 Problem. Where an agency's computing needs are more static and a migration to replacement hardware and/or software would be far more costly and time consuming than remediating existing systems, replacement makes no sense. Obviously budget constraints, in-house remediation capabilities, time limits and other factors will shape an organization's decision whether to replace its computer resources, remediate them, or simply ride out the Y2K wave and hope for the best.

---

[140] Y2K Committee Announces Survey Results Measuring Y2K Preparedness of Nation's Largest Utilities, found at http://www.senate.gov/~bennett/pr0612c98.html, site visited on October 21, 1998.
[141] DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998, at 3.

B. Curtis

6. *Abandonment*

Some non-compliant systems cannot be remediated, cost-effectively or at all, and replacement is also not a reasonable option, either because it is non-practicable or simply not possible under the time constraints. In these situations abandonment should be considered. The decision is much easier where the IT is not mission critical, but even mission critical systems may have to be abandoned and emergency work-arounds developed in some cases. The Senate Special Committee on the Year 2000 found that large power utility companies plan to "retire" or replace one out of four of their systems that are currently not Y2K compliant.[142] The DoD lists 128 of its 3,143 mission critical systems as destined for "planned terminations."[143]

E. SOLUTION ISSUES

1. *Time*

The is one of the most important issues bearing on solutions to the Year 2000 Problem. There is an unbridgeable gap between the amount of time required to fix or replace all of the computer-related technology that will be affected by the Year 2000 Problem and the time that remains before the arrival of January 1, 2000. There simply is not sufficient time remaining to complete all of the software remediation, hardware upgrades, processor replacements, and compliance testing before we can expect the millennial dates to begin taking their toll in the computer-driven world in which we live.

Writing for the Annual Institute of Computer Law in December of 1997, Dean Morehouse stated that "[a]lthough many more companies are in the midst of assessing the scope of their Year 2000 problem, the message is seemingly clear; many

---

[142] Y2K Committee Announces Survey Results Measuring Y2K Preparedness of Nation's Largest Utilities, found at http://www.senate.gov/~bennett/pr0612c98.html, site visited on October 21, 1998.
[143] DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998, at 3.

B. Curtis

companies simply will not be ready at the century date change."[144] Citing a September 1997 text, Morehouse quotes that "[r]eports vary, but there are published estimates that only 20% of medium and large sized companies have begun the process of converting their non-Year 2000 compliant code."[145]

The explanation for corporate America's early lethargy, if not outright apathy, in addressing the Year 2000 problem was described in 1993: "The reason that nothing is being done . . . is that the software industry isn't used to taking long-term preventative steps."[146] Since then some companies have reacted and begun to address the problem. Others resemble the doomed "deer in the headlights," frozen in fear, either overawed by the enormity of the task ahead, incapacitated by the potential for personal liability, or left to despair because it lacks the resources to effectively attack the problem.

The real risk associated with the efforts to avoid Year 2000 problems is that "[w]e're not good at delivering [computer] projects on time. Ask the question of several organizations and you'll find that most organizations find it difficult to deliver 50% of their projects on time."[147] "A good rule of thumb is that a software development project will take twice as long, and cost twice as much, as the original estimate."[148]

Senator Robert Bennett, chairman of the Senate's Special Committee on the Year 2000 Problem, recently concluded that "[w]e've reached the point where we cannot solve the whole problem. That is very clear. As a nation, as a government, we

---

[144] DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998), at 580-81.

[145] DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998), at 580-81, *citing* B. AUSTRIAN & T. PAGEL, MILLENNIUM MORASS (Montgomery Securities 1997), at 45.

[146] Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998, *quoting* Capers Jones, chairman at Software Productivity Research, Inc. Jones goes on to state, "I expect that most companies will not start worrying about the problem until 1999. . . . For some, this will be too late." *Id.*

[147] De Jager, Peter, *It's a People Problem*, found at http://www.year2000.com/y2kpeople.html, site visited on June 22, 1998.

[148] JOHN T. SOMA, COMPUTER TECHNOLOGY AND THE LAW (1983) at 94. The only constant from 1983 to the present in terms of software development is that the project will be over budget and late.

B. Curtis

cannot get this [entire] problem solved."[149]   The New York Times reports that the IRS still has to "convert a network of 80 mainframe computers, 14,000 minicomputers, 130,000 personal computers, and 100,000 desktop components to handle the [century-date] changeover."[150]   The Y2K remediation contractor for the State of Wyoming expects to take nearly three months (stretching at least through January 1999) to inventory and assess (but not actually fix) the 31 million lines of code in the State's computer systems.[151]   Some Y2K remediation companies have surveyed the enormity of the Year 2000 problem and have stated they expect to be performing Y2K repair services through the year 2005, moving from mission critical systems to less critical computer operations whose repair were postponed during the initial response.[152]

The typical organization will discover that 1-2 percent of its software must be modified to correct Y2K problems, but will have to analyze all of its code to find that small percentage.[153]   Manual methods are estimated to take one person working a normal work schedule an entire year to analyze and repair 100,000 lines of code. Organizations whose code makes greater use of date data in performing calculations and other functions can expect more than 2% of their software to require repairs. In today's computer-intensive service industry, many organizations have 10 million or more lines of code, which equates to 100 staff-years to remediate each organization's

---

[149] Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998, *citing* Sen. Robert Bennett, Chairman, Senate Special Committee on the Year 2000 Technology Problem, Address to the National Press Club, Washington, DC (July 15, 1998).

[150] Jeri Clausing, *IRS Must Address Millennium Bug Before Other Issues, Agency's Chief Says*, THE NEW YORK TIMES, May 8, 1998.

[151] " *The Titan Corporation Awarded State of Wyoming's Year 2000 Contract With Cap Gemini America as Subcontractor*, found at http://www.year2000.com/y2knews.html, site visited October 23, 1998.

[152] Leyla Kokmen, *State Picks Logix for 2000 Work Four-Month-Old Firm Lands $1 Million Work*, DENV. POST, May 1, 1998, at C01.

[153] Using a new repair program from Data Integrity, the consultant performing remediation work for Citibank was able to fix a system with more than 100,000 lines of code in a single day. The same repairs would have taken 30 days to make if the consultant had used the tools that were available before this program was released. "More programs and solutions continue to reach the market each week." Steve Hewitt (steve@ccmag.com), *Year 2000 Bug Part 1, The Challenge Ahead!* CHRISTIAN COMPUTING MAGAZINE, Volume 10 , Issue 9, Sep 1998, found at http://www.gospelcom.net/ccmag/articles/tele0998.shtml, site visited on October 23, 1998.

systems.[154] However, better and faster solutions are being crafted as the Year 2000 approaches and more time, energy and other resources are applied to making the changes necessary to avoid the computer problems. Early projections of the time required to remediate software are becoming obsolete as new remediation tools are developed. Some of these products can repair 100,000 lines of code per day.

The government's typical means of addressing a project deadline that cannot be met will not work in this situation. Saturday, January 1, 2000 is a fixed and unavoidable occurrence; even the government cannot stop time or slip that date to another date to provide the opportunity to deal with the myriad of non-compliant systems in a more leisurely--if ordered--fashion.

2. *Cost*

Cost continues to be one of the more thorny issues surrounding the Y2K problem, due to the difficulty in assessing an accurate figure of the number of systems requiring conversion, the uncertainty of the number of lines of software code which must be reviewed and fixed, and the rising costs of performing the required maintenance.[155] An additional problem is that these estimates appear to address only software programs and data files; they do not include the costs of remediating

---

[154] http://www.itl.nist.gov/div897/plan2000.htm, site visited on November 21, 1998.

[155] In any discussion of cost, it is important to identify what costs are being discussed, distinguishing between remediation costs intended to fix Y2K problems before they occur, and the costs that may be required to correct the harm to information systems that results from computer failures. The figures in this section are the former, but even so, do not distinguish between costs of remediating software and replacing existing computer resources with Y2K compliant technology. An additional cost to be considered is that of Y2K litigation, including actual expenses of maintaining the litigation and the cost of any judgments rendered. Some have concluded that early estimates of Y2K litigation expenses, in the hundreds of millions, may be too low. The Gartner Group has predicted "that litigation costs over Y2K service and product failures, both real and imagined, could soar to $1 trillion or more." http://www.itaa.org/Y2kadr1.htm, *citing Apocalypse Not*, TIME, June 1998, site visited on October 21, 1998. *See also* DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998), at 563 (Y2K remediation costs estimated at $200-600 million; litigation and liability costs estimated to exceed $1 trillion).

B. Curtis

embedded technology.[156] The ability to accurately predict remediation costs is greatly dependent upon the information managers have about the system; the more one knows about his IT, the easier it is to accurately gauge the time and resources requirements for making modifications and achieving compliance.[157] Published remediation estimates are generalizations made by industry analysts attempting to provide educated estimates for the user community to use in budgeting for repairs.[158]

In testimony before the House Subcommittee on Government Management, Information, and Technology on April 16, 1996, the research director for the Garter Group, a technology consulting firm, estimated that world-wide costs to fix the Y2K problem are as high as $600 billion.[159] He went on to explain that half of that figure ($300 billion) was attributable to U.S. remediation costs, and that 10% ($30 billion) of the U.S. figure represented what the federal government would spend on Y2K.[160] Members of the Information Technology Association of America (ITAA)[161] have also

[156] Published remediation cost estimates--almost without exception--indicate the estimated costs are for fixing "software," "code," "programs," "data files," or "systems." Note that each of the sources cited in this paragraph expresses remediation expenses as cost per line of code. Rarely is there any mention of embedded technology or microprocessors; one is left to conclude that embedded IT remediation costs have been overlooked or excluded from cost estimates. If so, this oversight is truly unfortunate as the final remediation costs for embedded technology may exceed the costs of software and data storage repairs.

[157] See DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, at section A.2.4, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998. Accurate remediation estimates will depend upon the program's complexity, the availability of documentation for the software, how experienced and skillful the remediation programmer is, the programmer's familiarity with the overall functionality of the software, the programming language the software is written in, and the remediation tools available. Id. The estimate should also take into consideration whether source code or only object code is available and whether the remediation team will be working on a "live" system or will be making the repairs off-line.

[158] Although estimates can vary widely, particular over time, many sources report figures generated by the Gartner Group when discussing Y2K remediation costs.

[159] Testimony of Kevin Schick, research director, The Gartner Group, before a hearing of the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight, Is January 1, 2000 the Date for a Potential Computer Disaster? (April 16, 1996).

[160] Still others have predicted that the federal government's Year 2000 costs will be "as much as $50 billion." Arnaud de Borchgrave, 'Millennium Bug' Battle a Case of Too Little, Too Late, THE WASH. TIMES, April 2, 1998.

[161] The Information Technology Association of America (ITAA) is composed of approximately 11,000 information technology manufacturers and service providers from across the United States. http://www.itaa.org/definition.htm, site visited on June 23, 1998.

B. Curtis

estimated the world-wide remediation costs at $600 billion.[162] Press accounts indicate the president has estimated government-wide Y2K remediation costs at only $5 billion,[163] but in a July 1998 address to the National Academy of Sciences he said that "[a]ll told, the worldwide cost will run into the tens, perhaps the hundreds of billions of dollars, and that's the cost of fixing the problem, not the cost if something actually goes wrong."[164] The Gartner Group estimated Y2K remediation efforts would cost the typical Fortune 500 company somewhere between $10 and $40 million.[165] Late in 1996, the Congressional Committee on Government Reform and Oversight noted that although the Department of Defense (DoD) had not yet completed its computer software inventory to determine exactly how many lines of code required conversion, the estimated cost to review and fix the DoD's estimated 358 million lines of code was between $1.02 and $8.52 per line, or somewhere between $358 million and $3 billion just for the DoD's fix.[166] In April of 1998, the Defense Science Board Task Force on Year 2000 stated that "[i]t is not possible to estimate the total cost of addressing the Y2K problem, because remediations have not been fully estimated, the costs of ongoing activities have not been clearly identified or segregated, and testing phase cost estimates do not exist yet."[167] Additionally, the Task Force pointed out that funds will be required for fixes after January 1, 2000, for temporary fixes (presumably of insufficiently repaired mission-critical systems and failed IT not previously identified as requiring

---

[162] http://www.itaa.org/y2kga.htm, site visited on November 21, 1998.

[163] Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4. The basis for the president's estimate is not clear, but this figure is less than 20% of what others have estimated for government remediation costs.

[164] Remarks by the President concerning the Year 2000 conversion, delivered to the National Academy of Sciences (July 14, 1998), and found at http://www.y2k.gov/new/presy2k.html, site visited on October 3, 1998.

[165] http://www.itl.nist.gov/div897/plan2000.htm, site visited on November 21, 1998. Early in 1996, the Gartner Group's world-wide repair bill estimate was reported to be somewhere between $300 and $600 billion. *Id.*

[166] Year 2000 Computer Software Conversion: Summary of Oversight Findings and Recommendations, H.R. Rep. No. 857, 104th Cong., 2d Sess. (1996), *citing* Tom Backman, MITRE Corporation, MITRE Assessment on the Effects of Two-Digit Years for the Year 2000, January 10, 1996.

[167] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) at 7.

B. Curtis

remediation) and to address those systems identified as "non-mission-critical" whose remediation was postponed.

The estimated costs of fixing non-compliant computer software have risen drastically from those projected 5 years ago when Year 2000 warnings were first sounded loudly and widely enough to generate any appreciable interest. Then, estimates ranged from $0.35 to $0.40 per line of code to convert non-compliant software to code which would properly process dates in and beyond 2000.[168] The estimators concluded that each Fortune 50 company would spend between $50 million and $100 million to fix their computer software for the next millennium.[169] By Spring of 1996, the Garter Group was predicting that it would "cost between $0.50 and $1 or more per line of executable code to analyze, modify, and test the software."[170] As late as November, 1998, the Garter Group was approximating repair costs at $1.50 per line of code, more than triple the estimates from 1993.[171]

Assuming remediation costs can be estimated with any degree of accuracy, the second hurdle is coming up with the colossal funds required. In its April 1998 Report, the Defense Science Board Task Force on Year 2000 explained the result of congressional direction on Y2K remediation budgeting:

> Currently expenditures to assure Y2K compliance will be contained within normal operating budgets. This "take-it-out-of-hide" approach seems to work well in those places where there is an ongoing program, including planned IT system replacements and upgrades. However, where no such designated funding is provided, performance accountability may suffer. . . .

---

[168] Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998, *citing* the conclusions of Ken Orr, principal at the Ken Orr Institute, and Larry Martin, president of Data Dimensions, Inc. These projections were made in 1993.

[169] Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993, and also found at http://www.year2000.com/archive/NFcw-article.html, site visited on October 20, 1998. De Jager found the costs of correcting this date change problem nothing short of mind-boggling. *Id.*

[170] http://www.itl.nist.gov/div897/plan2000.htm, site visited on November 21, 1998.

[171] http://www.itaa.org/y2kga.htm, site visited on November 21, 1998. Although inflation is often a factor in cost increases over time, it is hard to imagine that inflation, alone, could account for the three-fold increase in remediation costs.

B. Curtis

The "take-it-out-of-hide" approach also provides no resources for fixing "homeless" systems (those without a program office or budget) or for the replacement of legacy systems in financially strapped areas. . . . Perhaps most important, no funding mechanisms exist for system interface and "system-of-system" testing.[172]

The Task Force recommended the Secretary of Defense establish a "Y2K 'escape valve' fund" to be directly controlled by a newly created DoD Y2K executive (also recommended) who would manage the funds and make them available for the unfunded situations mentioned above.[173] The Task Force suggests the dollars for this fund could come from the money budgeted for the operational testing and evaluation of all DoD IT systems, not just those with Y2K issues, and if necessary, by imposing a tax on the DoD budget, or at least some of that budget.[174] The idea of creating a special tax to be used solely for Y2K remediation will undoubtedly appeal to some federal and state legislators. Nebraska has, in fact, already created a new tax to fund the Y2K conversion of its computers.[175] As the heat has been turned up on the Y2K issue, congressional attitudes towards remediation funding have relaxed. One press account captured the revised position: "Members of Congress have said they will allocate whatever money is necessary to keep the government functioning after Jan. 1, 2000."[176] On October 21, 1998, Congress passed and the President signed H.R. 4328, an omnibus Fiscal Year 1999 spending bill that promises $3.4 billion--$1.1 billion for DoD

---

[172] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) at 7. In so many words, the report seems to be saying that military organizations who had already budgeted to upgrade or replace their information technology should be able to absorb any additional cost of including Y2K compliance in the procurement. However, units who had no such plans and otherwise lack sufficient funds (undesignated or reprogrammable from less important projects) will not be able to achieve compliance without additional funds. And, where there are no funds, already available in the budget or provided supplementarily, DoD leadership should not expect those organizations to achieve Y2K compliance.

[173] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998), at 43.

[174] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998), at 43-44. Presumably the so-called "tax" would be a percentage of each military department's overall budget (or whatever portion of their budgets the tax is to come from) that the Secretary of Defense would seek congressional authorization to reprogram specifically for Y2K remediation.

[175] Year 2000 Computer Software Conversion: Summary of Oversight Findings and Recommendations, H.R. Rep. No. 857, 104th Cong., 2d Sess. (1996), note 21.

[176] Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4.

B. Curtis

and security agencies, and $2.3 billion for civilian agencies--in additional money to fund Y2K compliance efforts.[177] With the Year 2000 looming large on the horizon, it is not difficult to imagine where any near-term budget surpluses will be used.

3. *Personnel*

The Y2K software conversion effort is of such monumental proportions that there simply are not enough programmers in the labor force to adequately address the problem in the time that remains before 2000. Actually, the shortage of software programmers is not a new phenomena. In 1981 one writer discussing computer procurements described the problem as "the ever present problem of personnel shortages. For at least the last 15 years, and forecasted to continue through the 1980s, trained programmers have been a scarce resource."[178] Peter de Jager claims that "[t]he USA is the furthest along the path to implementing their solutions" but notes that the Information Technology Association of America estimates that the United States has 340,000 fewer computer programmers than required for the conversion task.[179] De Jager suggests that "power users," people within most organizations who have a rudimentary understanding of computer programming (without any formal training) and a natural proclivity for computers, need to undergo an abbreviated training program to give them the necessary skills to assist the organization's programming staff in converting computer systems before the turn of the century.[180]

---

[177] *Federal Spending Bill Includes $3.4B for Y2K Computer Problems at DOD, Other Agencies*, FEDERAL CONTRACTS REPORT, (BNA) Vol. 70, No. 15, 399, 406, October 26, 1998.

[178] JOHN T. SOMA, COMPUTER TECHNOLOGY AND THE LAW (1983), *citing generally* "Bernacchi, Davidson, & Grogan, *Computer System Procurement*, 30 Emory L.J. 395 (1981).

[179] De Jager, Peter, *It's a People Problem*, found at http://www.year2000.com/y2kpeople.html, site visited on June 22, 1998. Personnel shortages within the computer science industry, particularly in areas of software development and maintenance, is not a problem that is peculiar to this decade. Whether the problem is chronic or merely cyclical, we have had too few software programmers available to meet market demands at several times during the relatively brief "computer age."

[180] De Jager, Peter, *It's a People Problem*, found at http://www.year2000.com/y2kpeople.html, site visited on June 22, 1998. These "power users," according to De Jager, are the type of people who have taught themselves to write spreadsheet macros or have solved a Windows 95 problem on their own. *Id.*

B. Curtis

The personnel problem has generated a great deal of interest among the DoD's Command, Control and Communications (C^3) staffs--the Armed Forces premier computer technology elements.[181]   The Report of the Defense Science Board Task Force on Year 2000 highlights this concern:

> Several [C^3 organizations] expressed significant concern regarding recruiting and retaining the skilled IT civilian and military personnel needed in the DOD to address the Y2K problems during the next several years, the most critical time period.   It was clear to all that there is an IT employment environment with significant commercial demand, a national shortage of skilled personnel and escalating compensation packages.   This exists in the face of the recently announced Defense Reform Initiative (DRI).   The continued efforts to downsize the DOD, with the elimination of existing careers in military and civilian personnel IT and the DOD initiatives to outsource various IT functions exasperate the problem.[182]

Federal agencies have found the Y2K problem too large to fix with internal programming resources alone and have begun contracting out for Y2K services.[183] Some states have also found the Y2K problem too big to attack internally and are looking to commercial IT service providers to help them meet their compliance goals. Companies specifically created to address Y2K problems are springing up to meet both government and private sector requirements.   Colorado has hired an IT service contractor to fix Y2K problems in the computer systems used by the state's Department

---

[181] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) at 25.

[182] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) at 25. This portion of the Task Force's Report is based on briefings and discussions with C^3 representatives from "Defense Information Systems Agency (DISA), Joint Chiefs of Staff (JCS/J6), OPNAV (N6), Head Quarters Marine Corp (HQMC) (C^4I), Air Force Program Executive Office (AFPEO/C^3), Airborne Warning and Control System (AWACS), Assistance Secretary of Defense (ASD C^3I), Joint Tactical Information Distribution System (JTIDS) and the E6-B program." *Id.* at 24.

[183] The U.S. Agency for International Development recently awarded a "technology management" contract, with a one-year base period and four option years, potentially worth $192 million, to Computer Sciences Corp. The "technology management" includes providing Y2K improvements as a component of managing the agencies computing resources. *Computer Sciences Gets U.S. Job*, WALL ST. J., June 17, 1998, at A18. The information technology career field has become so competitive in the past months that the Department of Labor's Internet Job Bank now includes a special section specifically for employers and job seekers in the Year 2000 information technology industry. *See* http://it.jobsearch.org/, site visited on November 17, 1998. The federal government is not alone in contracting out for a Y2K solution. Australia is planning for information technology contractors to perform an audit of Y2K compliance within its federal departments and agencies. Additionally, the contemplated contracts will provide the government with a wide spectrum of Y2K legal advice, including issues of liability for government service providers and a release of readiness information. Ian Davis, AUSTL. FIN. REV., May 23, 1998, 1998 WL 12564955.

of Human Services and the Department of Revenue. The $1 million contract (of an expected $37 million total cost) was awarded to Logix Solutions, a four-month old firm which has already been acquired by a larger company.[184] Indiana, which has already budgeted $53 million for Y2K remediation efforts, reports it will need at least $10 million more to fix government IT systems.[185] Wyoming has awarded a $34.1 million contract to The Titan Corporation to provide statewide Year 2000 services for government computer systems.[186] The contract covers the first two phases of the work, which call for an inventory and assessment of all state information systems. The third phase, not included in the $34.1 million contract, will involve the actual remediation and testing of the State's systems.

III. GSA'S YEAR 2000 WARRANTY

As government agencies became aware of the need to address the Year 2000 issue when contracting for the procurement of IT, they faced great difficulty because neither the FAR nor any federal statutes had established a single, clear set of requirements for procuring computer technologies which would accurately process dates into the next century. Agencies that were aware of the issue were ready enough to procure items that were "Year 2000 compliant," but without a standard, government-wide definition of compliance, individual procuring activities were left to either write specifications which defined the term as they deemed most appropriate, borrow definitions from other contracting activities which had previously addressed Year 2000 compliance, or simply include a specification that the subject product or system be

---

[184] Leyla Kokmen, *State Picks Logix for 2000 Work Four-Month-Old Firm Lands $1 Million Work*, DENV. POST, May 1, 1998, at C01.

[185] *Expenses Rising for Y2K Fix*, CHICAGO TRIBUNE, October 21, 1998, found at http://www.chicagotribune.com/splash/article/0,1051,SAV-9810210047,00.html, site visited on October 21, 1998.

[186] *The Titan Corporation Awarded State of Wyoming's Year 2000 Contract With Cap Gemini America as Subcontractor*, found at http://www.year2000.com/y2knews.html, site visited October 23, 1998. The inventory and assessment will cover the State's "mid-range, desktop, and selected mainframe applications." *Id.*

B. Curtis

"Year 2000 compliant" without providing any clarifying details. Multiple, widely-varying requirements arose, some of which were ineffective in addressing compliance and others which set out overly demanding--and potentially unenforceable--requirements.[187] This confusion-laden contracting environment was exacerbated wherever federal agencies were required to interface their systems with those of other agencies, contractors, or vendors. A contractor's product might meet the procuring agency's compliance definition and yet not be able to properly operate in combination with the other agency's system due to that agency having required its IT contractors to meet a more stringent compliance standard.[188]

Whatever uneasiness government contracting personnel experienced with this uncertainty of terms, the difficulties faced by contractor personnel were multiplied by the number of government agencies with whom they were engaged.[189] A single contractor would feasibly be required to attain numerous, differing standards--all labeled "Year 2000 compliant"--while concomitantly facing differing degrees of liability risk because of varying warranty provisions among its government contracts. Some federal agencies specified requirements in terms that were impossible or impracticable to meet, such as insisting that the procured IT perform "fault-free" date handling.[190]

---

[187] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. Some agency needs were stated in language which was "impossible to perform," potentially leaving the agency in the position of having its valid requirements go unfulfilled because they were expressed in specifications which far-exceeded the requirements. *Id.*

[188] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[189] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. "Agencies exchanging data with other government entities as well as software manufacturers were understandably concerned with having to meet what, quite literally, could have been hundreds of Year 2000 compliance standards." *Id.*

[190] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 5.

B. Curtis

This lack of a single compliance definition or standard and the vagueness it produced was equally troubling in the area of IT warranty clauses. Here, again, there was no standard clause to be used throughout the federal government to warrant an IT product's or system's ability to function properly up to and into the next century. Some warranty clauses also imposed unrealistic requirements upon contractors, apparently requiring the contractor to certify Year 2000 compliance for IT products supplied by other contractors in addition to those it would supply.[191] "The degree of risk the vendors were being asked to assume had a direct and predictable impact on pricing."[192] Understandably, contractors were unhappy with the Y2K contracting environment and resisted what they saw as unreasonable government requirements.[193] Both government procurement officials and IT contractors/manufacturers were in desperate need for procurement guidance to provide a single, uniform standard to be used when requiring Year 2000 compliant IT.

At the request of the Chief Information Officers Council, GSA took the lead in drafting FAR provisions and warranty clauses to address the Year 2000 problem in government procurement. GSA, the government's largest provider of IT supplies and services, worked with the Office of Management and Budget (OMB) and the Chief Information Officers Council Subcommittee on the Year 2000, forming an "Interagency

[191] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. "Broad statements requiring the contractor's product to process data/time information accurately (regardless of the source of the data), or that Year 2000 output data will successfully operate on any connected system, imposes nearly unlimited risk on the contractor." *Id.* at section 2.5.2.

[192] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. "When faced with unreasonable specifications/requirements, vendors will either choose not to propose, or price that assumed risk into the offer." *Id.* at section 2.5.2.

[193] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (September 18, 1996). Mr. Kenney, who was involved with negotiating the language of GSA's Year 2000 warranty clauses on behalf of the Information Technology Association of America (ITAA), wrote that "[i]n many instances the Government's demands for Year 2000 warranties or similar guarantees have met with strong resistance from vendors on technical, practical, and legal grounds." *Id.*

B. Curtis

Committee on the Year 2000," to develop a Year 2000 Warranty clause that would address the government's Y2K concerns in buying new IT items and at the same time be reasonable in the requirements it levied upon government contractors. Considering the huge volume of commercial IT products purchased by federal agencies off the GSA's Federal Supply Schedules,[194] it would make sense for the GSA to develop warranty language to address Y2K issues. The "Interagency Committee" developed five prototype versions of the Year 2000 Warranty clause and placed them on the Internet in May, 1996, allowing agencies and industry to comment on the prototypes.[195] Based upon the comments, a single draft version was created and provided to agencies and industry.[196] After months of meetings and negotiations between the "Interagency Committee" and representatives of the government and the IT industry,[197] the committee produced two versions of a warranty, one for the procurement of commercial supply items and the other for the procurement of non-commercial supply items.[198] The

[194] Sales of IT supplies and services via GSA's Federal Supply Schedules continues to rise as January 1, 2000 approaches. *GSA Projects IT Sales Will Reach $6B in FY 1999,* FEDERAL CONTRACTS REPORT, (BNA) Vol. 70, No. 21, p 604, December 14, 1998. Fiscal Year 1997 IT spending on GSA's Schedules alone was $2.8 billion, which increased 68% in FY 1998 to $4.7 billion. Based on the fact that federal agencies have purchased as much in IT services during the first two months of FY 1999 as was acquired over a six month period in FY 1998 ($519 million), GSA predicts that total IT spending via their schedules will reach $6.1 billion in FY 1999. *Id.*

[195] FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[196] FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[197] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at sections 1.1 and 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[198] http://www.itpolicy.gsa.gov/library/yr2000/y201toc1.htm (August 1996), and quoted in its entirety in *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests,* 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (September 18, 1996). Note that the original version of GSA's Year 2000 Warranty clauses are no longer available at this site. Furthermore, GSA representatives indicate that the version of the clauses included in the GSA White Paper on Application and Implementation of Year 2000 Federal Acquisition Regulation Guidance (found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998) was not the version originally posted on the GSA Information Technology Policy Internet page. Rather, the version that was current at the time the Paper was published was included, reflecting any changes which had been made as GSA continued to refine the warranty language. Electronic mail titled "Re: Y2K Questions" from Dave Middledorf, <dave.middledorf@gsa.gov> (September 23, 1998) (on file with author). Both Dave Middledorf and Susan Hinden indicated that they were unable to locate an official record copy of the clause in the form originally posted on the Internet. Electronic mail titled "Re: Year 2000 Warranty: Original Version" from Susan Hinden, <susan.hinden@gsa.gov> (September 14, 1998) (on file with author); and electronic mail titled "Re: Y2K Questions" from Dave Middledorf, <dave.middledorf@gsa.gov> (September 23, 1998) (on file with

warranty clauses were posted on GSA's home page late in August of 1996.[199] Since

then, the clauses have been modified to conform to the final version of the FAR's

definition of Year 2000 compliance.[200]

---

author). Dave Middledorf, a GSA Information Technology Policy Analyst, located a non-official, personal copy of the original version of the clauses and provided a facsimile to the author, advising that the original version (having been revised and republished) was "not included in the final FAR rule and should only be used as a sample of clauses for agencies to use." Facsimile from Dave Middledorf (202-501-1551) (October 20, 1998) (on file with author). The author notes that this facsimile version is identical to the version of the warranty clauses included in the FAR Information Technology Committee Report on FAR Case 96-607, dated October 28, 1996. Therefore, references to the original version of the GSA Year 2000 Warranty clauses will be cited to *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[199] The original version of the warranty clauses read as follows:

Year 2000 Warranty - Commercial Supply Products

The contractor warrants that each hardware, software, and firmware product delivered under this contract and listed below shall be able to accurately process date data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, including leap year calculations, when used in accordance with the product documentation provided by the contractor, provided that all listed or unlisted products (e.g. hardware, software, firmware) used in combination with such listed product properly exchange date data with it. If the contract requires that specific listed products must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed products as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract, provided that notwithstanding any provision to the contrary in such commercial warranty or warranties, the remedies available to the Government under this warranty shall include repair or replacement of any listed product whose non-compliance is discovered and made known to the contractor in writing within ninety (90) days after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.

Year 2000 Warranty - Non-Commercial Supply Products

The contractor warrants that each non-commercial item of hardware, software, and firmware delivered or developed under this contract and listed below shall be able to accurately process date data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, including leap year calculations, when used in accordance with the item documentation provided by the contractor, provided that all listed or unlisted items (e.g. hardware, software, firmware) used in combination with such listed item properly exchange date data with it. If the contract requires that specific listed items must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed items as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of any general warranty provisions of this contract, provided that notwithstanding any provision to the contrary in such warranty provision(s), or in the absence of any such warranty provision(s), the remedies available to the Government under this warranty shall include repair or replacement of any listed item whose non-compliance is discovered and made known to the contractor in writing within ninety (90) days after acceptance. Nothing in this warranty shall be construed to limit any

B. Curtis

A. TWO VERSIONS OF THE CLAUSE

The final versions of the GSA Year 2000 Warranty clause for commercial and non-commercial supply items were revised August 22, 1997 and are published on GSA's IT Policy page on the Internet.[201] The text of those versions is quoted and examined in the following paragraphs.

1. *Commercial Supply Items*

Year 2000 Warranty--Commercial Supply Items

The contractor warrants that each hardware, software, and firmware product delivered under this contract and listed below shall be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it. If the contract requires that specific listed products must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed products as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract, provided that notwithstanding any provision to the contrary in such commercial warranty or warranties, the remedies available to the Government under this warranty shall include repair or replacement of any listed product whose non-compliance is discovered and made known to the contractor in writing within ninety (90) days after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.[202]

rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.

Originally available at http://www.itpolicy.gsa.gov/library/yr2000/y201toc1.htm (August 1996), and quoted in its entirety in *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[200] Both the Commercial Supply Items and Non-Commercial Supply Items clauses are available at http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm, site visited on September 16, 1998; however, only the final version of the clauses are available.

[201] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[202] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998. There are two notes accompanying the commercial supply item clause:

Note for solicitations and new contracts: The solicitation should describe the existing computer system or the products (i.e., firmware, middleware, etc.) that will be used with the commercial products and systems being acquired, and as appropriate, whether those existing systems and products are Year 2000 compliant, and any efforts currently underway to provide this capability.

Note for existing contracts: It is recommended that agencies negotiate modifications to existing contracts for acquisition of new products using the above clause as a guide. Prior to modifying the contract, the

B. Curtis

2. *Non-Commercial Supply Items*

Year 2000 Warranty--Non-Commercial Supply Items

The contractor warrants that each non-commercial item of hardware, software, and firmware delivered or developed under this contract and listed below shall be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it. If the contract requires that specific listed items must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed items as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of any general warranty provisions of this contract, provided that notwithstanding any provision to the contrary in such warranty provision(s), or in the absence of any such warranty provision(s), the remedies available to the Government under this warranty shall include repair or replacement of any listed item whose non-compliance is discovered and made known to the contractor in writing within ninety (90) days after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.[203]

---

project team must ensure (1) that performance is possible considering the characteristics of the existing products, (2) the suppliers' agreements with the integrator will allow this work to be performed, (3) cost of performance will not be prohibitive, and (4) that the contractor will agree to the modification (should be a bilateral modification). The Government may elect to acquire versions of those products that warrant accurate performance in the processing of date and date related data. *Id.*

[203] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998. There are also two notes accompanying the non-commercial supply item clause:

Note for solicitations and new contracts: The solicitation should describe the existing computer system or the items (i.e., firmware, middleware, etc.) that will be used with the software and systems being acquired, and as appropriate, whether those existing systems, items, and software are Year 2000 compliant, and any efforts currently underway to provide this capability.

Note for existing contracts: It is recommended that agencies negotiate modifications to existing contracts for acquisition of new items using the above clause as a guide. Prior to modifying the contract, the project team must ensure (1) that performance is possible considering the characteristics of the existing items, (2) the suppliers' agreements with the integrator will allow this work to be performed, (3) cost of performance will not be prohibitive, and (4) that the contractor will agree to the modification (should be a bilateral modification). The Government may elect to acquire versions of those items that warrant accurate performance in the processing of date and date related data. *Id.*

B. Curtis

B. Features of the Clause

1. *Comparison of Two Versions*

While the Commercial and Non-Commercial Supply Items versions of the Year 2000 Warranty clause are nearly identical, there are two substantive differences between them. First, in addition to "delivered" items that are covered under the commercial clause, the non-commercial clause also covers items "developed" under the contract.[204] The reference to items *developed* is largely intended to extend coverage to items of custom-designed software.[205] Second, the commercial clause incorporates the terms and limitations of the contractor's standard commercial warranty by reference; whereas, the non-commercial clause simply states that the terms and limitations of the contract's general warranty provisions will also apply to Year 2000 compliance. This difference is merely reflective of the typical differences in warranties between commercial and non-commercial item contracts.[206] A contract for non-commercial items would not include the type of standard commercial warranty that would be found in most contracts for commercial items; instead, it will normally have a general warranty provision covering all aspects of the contract. Both versions contain "notwithstanding any provision to the contrary" language preserving to the government the minimum remedies of repair or replacement so long as the government notifies the contractor of the non-compliance in writing within 90 days after acceptance of the item. These differences reflect the drafters' intent to minimize the inclusion of additional terms by subsuming the Year 2000 compliance coverage under the normal warranty provisions of the particular contract rather than creating additional terms to specifically address the

---

[204] See http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[205] See *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 Gov't Contractor (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[206] This commercial/non-commercial difference is also reflected in the use of the term "product" in the commercial version and "item" in the non-commercial version. The difference is more one of form than substance.

B. Curtis

Year 2000 compliance issue. Relative to the terms of Year 2000 compliance, the two clauses are identical.

2. *Voluntary Use*

Both versions of the clause are available for use by federal agencies[207] purely on a voluntary basis;[208] there is no requirement to include either of these clauses in government IT solicitations or contracts. In fact, the introductory language accompanying the clauses on GSA's IT Policy page on the Internet explain that the clause is not recommended where:

> (1) the requirement will not continue to exist after December 31, 1999, or (2) the agency has decided to accept offers from vendors that do not have the needed Year 2000 compliant products, but will be required under the contract to upgrade the information technology items to be Year 2000 compliant by a suitable date in advance of the year 2000.[209]

If the clause were included in the first situation, the government would almost certainly pay more for the items than was necessary, either in the form of more costly components, software development or product testing, or in the form of a price increase to cover the additional risk the contractor must assume. Inclusion under those facts would open the government to challenges that it was over specifying or overstating its requirements. Including the clause in the second situation would unduly restrict competition, limiting bidding to those contractors whose products were already compliant when compliance could be achieved at a later, acceptable date. Where government requirements are not so immediate as to require the IT to be compliant upon delivery, agencies can maximize competition and get the best value by allowing

---

[207] The clauses are available on the Internet and could actually be used by anyone desiring assurance that what they are contracting to buy will be able to function properly in the next century.

[208] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998. "This clause is recommended for voluntary use by Federal agencies in their solicitations and contracts for Year 2000 compliant software, hardware, and systems . . . ." *Id.*

[209] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

contractors with non-compliant products to compete so long as the items will be made compliant before they are required to process millennial dates.

When the "Interagency Committee on the Year 2000" was revising the FAR to define "Year 2000 compliant" and limit IT acquisitions to Year 2000 compliant items, it also had intended to make the GSA Year 2000 Warranty a part of the FAR Part 52 warranties.[210] Although the DAR Council originally concurred in this decision, the Council later determined that it was inadvisable to add another warranty to the FAR.[211] To continue to make Year 2000 warranty language available to other federal agencies, GSA updated the warranty to reflect changes made in the FAR compliance provisions and published the final Year 2000 Warranty clauses on the GSA IT Policy page on the Internet to be used on a voluntary basis.[212] Even though use of the clause is strictly voluntary, GSA notes that "the warranty provision has proven extremely valuable and is currently in use in over $5 billion of Federal IT contracts."[213]

---

[210] FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996; confirmed by telephonic interviews with Dave Middledorf, GSA Information Technology Policy Analyst (October 16, 1998) and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

[211] Telephonic interviews with Dave Middledorf, GSA Information Technology Policy Analyst (October 16, 1998) and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998). *See also,*
Memorandum from Edward C. Loeb, Chairman, Civilian Agency Acquisition Council , to CAAC Members (June 11, 1997) (found in Case File 96-607 at the FAR Secretariat). "In addition to the editorial changes to the Year 2000 definition, the DARC disapproved the issuance of the warranty clauses as an interim rule. The DARC maintained that FAR 46 provides adequate guidance on warranty clauses, therefore, the proposed warranties should not be incorporated into the Federal Acquisition Regulation." *Id.*
The rationale for the DAR Council's position is discussed in a little more detail below in the section on effectiveness and suitability of the FAR Year 2000 compliance provisions.

[212] Telephonic interviews with Dave Middledorf, GSA Information Technology Policy Analyst (October 16, 1998) and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

[213] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.1, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. The $5 billion number was published in August of 1997 barely a year after the clauses were originally published on the Internet. Presumably the final version of the warranty clauses have been used in IT contracts totaling an equally large number of contract dollars.

B. Curtis

3. *Scope of Clauses*

The warranty is expressly limited to IT products: "hardware, software, and firmware product[s],"[214] and does not apply to contracts for IT services. Where a contract for the purchase of IT products includes a provision for installation services, such services would typically be considered incidental to the purchase and would not dilute a contractor's obligation simply because the product's non-compliant performance resulted from improper installation.[215] Furthermore, the warranty applies only to "listed" items, meaning only those that the contractor specifically designates as being Year 2000 compliant in response to the procuring agency's specifications. It is because of this warranty feature that the explanatory language accompanying the warranty specifically states "[t]he clause may be used when some but not all of the products being acquired are required to be Year 2000 compliant"[216] because, by its terms, the warranty will only apply to the appropriate ("listed") items. Clearly this facet of the warranty places a burden on both the contracting officer and the government contractor to ensure that all the items required to be Year 2000 compliant--and *only* those items-- are listed as such in the contract. The explanatory language reminds contracting officers to secure an express warranty covering all "unlisted" items and providing for repair or replacement of all items discovered to be defective within a reasonable period of time after acceptance.[217]

The warranty is appropriate for use in solicitations and the resulting contracts, as well as in existing contracts. Because the terms as written apply only to products, such

---

[214] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[215] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 12.

[216] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[217] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998, *citing* FAR Part 12.

B. Curtis

as "hardware, software, and firmware,"[218] the warranty is not appropriate for use in IT service contracts in its current form. The notes accompanying the warranty clauses advise agencies to insure their solicitations include a description of any computer system or computer-related items they intend to use with the IT being acquired, indicating whether the other items are Year 2000 compliant or are projected to be made so. This is laudatory advice, yet it does too little towards insuring that agencies will meet the presumed goal: successful interoperability. Because of the different technical solutions for achieving Year 2000 compliance, it is insufficient to merely advise a contractor whether or not the additional computer-related products are compliant. If an agency's project team wants to be sure the items being acquired will operate successfully with the other items it is currently operating (or is acquiring from different IT contractors), the team must provide sufficient technical information to insure that the contractor's Y2K solution will be compatible.

In existing contracts, the notes advise, agencies should consider negotiating a modification to the contract to include the compliance warranty.[219] Factors to be weighed in determining the advisability of including the warranty include considering whether 1) compliance is possible in view of the item's current characteristics, 2) agreements between the supplier and integrator will allow the required modification efforts, 3) obtaining compliance would be cost-prohibitive, and 4) the contractor is willing to add the compliance warranty.[220] These factors, taken as a whole, focus on whether modifying an existing contract would be a prudent decision from a purely business judgment perspective.

---

[218] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[219] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[220] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

It may not be possible to make some products compliant, whether because of physical design limitations of the product or because subcontracts do not provide for the required work. Where compliance is possible, the cost of compliance may drive up the contract price so sharply as to make it a poor business decision for the agency to request the modification. The last factor is, perhaps, the most difficult. If the contractor is unwilling to modify the contract and thereby become obliged to both make compliant products and warrant their compliance, the note provides no solution. It simply states that any modification "should be a bilateral modification."[221] The agency could unilaterally modify the contract pursuant to the Changes clause[222]--for non-commercial item[223] contracts--to require that the items be Year 2000 compliant, or the agency could terminate the contract for convenience,--for either commercial or non-commercial item contracts.[224] Keep in mind that the GSA warranty clause is voluntary; an agency need not chose between including the warranty via bilateral agreement or the Changes clause, or terminating the contract where modification is not possible.

The only other option offered in the accompanying notes is for the agency "to acquire versions of those products" that *are* compliant.[225] This option assumes the contractor has a varied product line, some of which are non-compliant (and were contracted for by the agency) and others which are compliant (which might be substituted by contract modification), and that the latter products would satisfactorily fulfill the government's requirements. Where contractors' product lines present such an option, agencies would do well to consider a modification to substitute compliant products for non-compliant ones for a number of reasons. The contractor will already

---

[221] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.
[222] FAR 52.243-1.
[223] Contracts for commercial items do not include the Changes clause. *See* FAR 52.212-4, Contract Terms and Conditions--Commercial Items.
[224] FAR 52.249.
[225] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

have included the costs of compliance into the price of the products, so that there need not be any premium charged for altering a non-compliant product. Furthermore, there is less likelihood of experiencing the delays often associated with making product alterations if the contractor already manufactures or stocks compliant versions of its product. Lastly, if the contractor is already marketing compliant versions of the product, it has probably already subjected that product to Y2K testing and found the product reliable. A modified product would have to be tested, meaning even greater cost increases and delivery delays, and the agency would have more doubts about a modified-product's Y2K performance than it would a product that was specifically designed, manufactured, tested, and marketed to be Y2K compliant.

4. *Warranted Standard of Performance*

The clause does not refer to Year 2000 compliance; rather, it simply warrants a particular level of performance that the contractor's products will achieve.[226] The standard of performance warranted in the clauses mirrors that used in the final "Year 2000 complaint" definition in the FAR: "shall be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations."[227] This standard differs in two respects from the original version of the GSA warranty: 1) "time" was added to yield "date/time data," and 2) the phrase "and the years 1999 and 2000" was inserted.[228] Both these changes are discussed

---

[226] While the term "Year 2000 compliant" is not found in the language of the warranty itself, the explanatory language accompanying the clauses clearly indicates the purpose for warranting the standard of performance: "This clause is recommended for voluntary use by Federal agencies in their solicitations and contracts for **Year 2000 compliant** software, hardware, and systems comprised of commercial information technology products . . . ." http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998, *emphasis added.*

[227] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998; *see also* FAR 39.002.

[228] See the original version in *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996; and the final version at

B. Curtis

below in the section on the FAR Year 2000 compliance provisions. The standard itself is also discussed in detail below in the analysis of FAR 39.002, which also defined "Year 2000 compliant." Unlike the compliance requirement in the FAR, the warranty addresses the interoperability of the acquired products in situations where the contract requires the products to function as a system. "If the contract requires that specific listed products must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed products as a system."[229] Any products that were "listed" but not specifically required to perform together as a system are free from this "system-compliance" requirement.

There is an exception to the warranty where the acquired products will interface with other IT. In that situation, the acquired products are warranted to accurately process date/time data only "to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it."[230] This exception would protect the IT contractor where the interfacing IT is not compliant. It would provide that same protection when the interfacing IT is compliant, but is unable to properly exchange date/time data with the warranted product. Such exchange problems may result when different technical solutions have been employed to attain Y2K compliance in the "other information technology" than was used in the warranted product. As an example, the warranted product may use a four-digit year date field while the "other information technology" may use a windowing technique. The difference in technical solutions could be expected to make it impossible for the two systems to interface properly, and the exception would save the IT contractor in this situation.

---

http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[229] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[230] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

The original version of the warranty clause for commercial items included a similar, although differently-worded, exception: the acquired products are warranted to accurately process date data "provided that all listed or unlisted products (e.g. hardware, software, firmware) used in combination with such listed product properly exchange date data with it."[231] Here also the warranty has been revised to track with the language selected for the final FAR rule defining Year 2000 compliant.[232] In addition to the interoperability exception, the original warranty clause contained another proviso, warranting the product's date-handling performance only "when [the product is] used in accordance with the product documentation provided by the contractor."[233] This portion of the warranty was removed altogether as GSA sought to define compliance as that term had been defined in the FAR

5. *Inclusion of Standard or General Warranty Provisions*

Both of the GSA Year 2000 Warranty clauses expressly reference other warranties, applying provisions of those warranties to the GSA warranty. In a commercial supply item contract, the "duration of [the GSA] warranty and the remedies available to the Government for breach of [the GSA] warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract."[234] This feature of the GSA warranty complies with the Federal Acquisition Streamlining Act's requirement for contracting officers to take advantage of commercial warranties[235] and comports with the philosophy behind commercial products contracting: the government will fulfill many of its needs

---

[231] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 Gov't Contractor (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.
[232] See FAR 39.002.
[233] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 Gov't Contractor (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.
[234] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.
[235] 41 U.S.C.d264 note; *see also* FAR 12.404(b) "Express warranties."

B. Curtis

most economically and satisfactorily when its purchases in the marketplace much like other buyers, acting as nearly as possible like a commercial entity. A contractor's standard commercial warranty for a given product might include disclaimers as part of its "terms and limitations." Commercial warranties frequently disclaim the warranty of merchantability and the warranty of fitness for a particular purpose.[236] The GSA warranty does not depend upon either of these commercial warranties for its vitality; nonetheless, the government agency should consider how such a disclaimer could limit agency options if the product failed for some reason unrelated to the Year 2000. This is especially important because FAR 52.214-4 "Contract Terms and Conditions-- Commercial Items" automatically includes express warranties of merchantability and fitness for a particular purpose in government commercial item contracts[237] unless the contract specifically disclaims them. In a contract for items containing embedded IT, which are not currently covered by the FAR's Year 2000 compliance requirements, one of these warranties might provide the legal basis for a government remedy just as the Year 2000 Warranty would if included in an IT contract.

In contracts for non-commercial supply items, the duration of the GSA warranty and the government's breach remedies "shall be as defined in, and subject to, the terms and limitations of any general warranty provisions of this contract." In this case, the general warranty functions just like the contractor's standard commercial warranty in the commercial item contract: the general warranty provides the structure for the GSA warranty regarding duration, remedies, terms and limitations. If the particular contract

---

[236] FAR 12.404(b)(2) specifically recognizes this commercial reality and provides the required government response:
In some markets, it may be customary commercial practice for contractors to exclude or limit the implied warranties contained in 52.212-4 in the provisions of an express warranty. In such cases, the contracting officer shall ensure that the express warranty provides for the repair or replacement of defective items discovered within a reasonable period of time after acceptance. *Id.*
[237] FAR 52.212-4(o) "Warranty. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract." *Id.*

B. Curtis

non-commercial item contract contains no general warranty provisions, then the government agency will have the minimum rights declared in the GSA warranty.

6. *Government's Minimum "Repair or Replace" Remedy*

Regardless of whether the contract is for commercial products or non-commercial items, the applicable GSA Year 2000 Warranty clause provides the government with a set of minimum rights.[238] These minimum rights are the fallback remedies when there is no general warranty (non-commercial item contract) and endure even if the contractor's standard warranty purports to otherwise limit government remedies (commercial item contract). In either event, the government will have ninety (90) days after accepting the item in which do discover any problem and notify the contractor. Upon notification, the contractor is required to either repair or replace the item, assuming it is indeed covered by the GSA warranty. Even where the contractor's standard commercial warranty limits the warranties of merchantability and fitness for intended purpose--or excludes them altogether--FAR 12.404(b)(2) requires the "repair or replace" option.[239] One pair of commentators interprets the commercial clause's requirement that "the remedies available to the Government under this warranty shall include repair or replacement"[240] as allowing the contractor "some flexibility"[241] in providing the government contractual remedies. "For example, a contractor that offers repair, replacement, *or refund* as part of its standard commercial warranty would presumably be in compliance with both the [GSA Year 2000 Warranty] clause and FAR

---

[238] *See* http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.
[239] FAR 12.404(b)(2).
[240] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.
[241] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 14.

B. Curtis

12.404(b)(2) since the Government's remedies would 'include' both repair and replacement."[242]

Both clauses end with a notice that "[n]othing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance."[243] It is not clear what harm this section of the clauses is intended to protect the government from suffering.[244] It may have been included to indicate that the listed hardware, software and firmware products were warranted not only for Year 2000 performance, but also to meet whatever standards apply to every other product purchased under the contract. If any of the "listed" hardware, software or firmware met the Y2K performance standard, but were found to be defective in some other respect, the standard commercial or general warranty would still apply to that defect. Since the warranty applies only to listed IT products, and then only warrants their performance relative to the Year 2000, this statement appears to be unnecessary.

---

[242] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 14, *emphasis added*.

[243] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[244] The language could be viewed as an attempt to protect the government when the general warranty or standard commercial warranty provides greater rights (e.g. a 120-day notice requirement for defects) than the GSA warranty, but only when the defect is something other than a Year 2000 performance problem. The balance of the clauses' language simply does not permit such a situation; the GSA warranty provides a coverage floor, specifically for when the contract's provisions provide lesser coverage. When the defect is something other than a Year 2000 performance problem, the defect is covered by the general warranty or the standard commercial warranty.

The GSA warranty clauses specifically apply by their terms to hardware, software, and firmware products. Anything else (other than hardware, software, or firmware) acquired pursuant to the same contract would not be covered by the Y2K warranty in the first place; rather, they would be covered by the general warranty or standard commercial warranty. Regarding the hardware, software, and firmware products which are covered by the GSA warranty, the clauses reference the general warranty or standard commercial warranty in the contract for terms, limitations, duration and remedies. If the contract includes a general warranty or a standard commercial warranty that provides the government with greater rights or remedies (the 120-day notice requirement) than the minimum rights contained in the GSA Year 2000 Warranty (the 90-day notice requirement), the government may avail itself of those greater rights and remedies. If the other warranty in the contract provides lesser rights or remedies (e.g. a 45-day notice requirement) than those in the GSA warranty, the government will retain the minimum rights expressed in the GSA warranty.

B. Curtis

C. Issues

The GSA Year 2000 Warranty clauses made great strides towards providing necessary stability in government IT acquisitions, both for government agencies and IT contractors. Still, in the shadow of these clauses several issues remain for consideration. Firstly, the warranty does not specify any particular method for attaining Year 2000 compliance; rather, the clauses simply delineate the performance requirements that must be attained to fulfill the warranty. No particular technical solution is required to meet the standard; any of those solutions described above, or another developed by the contractor, might be sufficient to meet the standard. Some agencies may not care how compliance is achieved, so long as the delivered product meets the warranted standard of performance. This would be more likely where the acquired IT will not interface with other IT, or will do so without the need to exchange date data. Additionally, agencies who include the Year 2000 Warranty clause in their contracts may also include specifications regarding the method of compliance, identifying the technical solution to be employed or identifying the type of date-storing convention that must be observed.

Secondly, there is no version of the clause designed to be used in IT service contracts. The clauses were designed with commercial and non-commercial item contracts in mind, rather than service contracts. Under the commercial items clause "[t]he contractor warrants that each hardware, software, and firmware *product delivered* . . . shall be able to accurately process date/time data," and under the non-commercial items clause "[t]he contractor warrants that each non-commercial *item* of hardware, software, and firmware *delivered or developed* . . . shall be able to accurately process date/time data."[245] The terms of warranty clauses simply do not anticipate service contracts which might be used to modify or remediate the government's IT. However,

---

[245] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998, *emphasis added.*

B. Curtis

with very little effort the warranty clauses could be modified so as to apply to IT service contracts. It is possible that some agencies have used the clause, as is, in IT service contracts to establish the performance requirements relative to the Year 2000, regardless of whether the main purpose for the contract was Y2K remediation.

Thirdly, it is not clear whether or not the clauses apply to embedded technology. The warranty extends to "each hardware, software, and firmware product delivered" or "each non-commercial item of hardware, software, and firmware delivered or developed."[246] Embedded technology typically take the form of microprocessors--which would qualify as firmware--and would be encompassed in the definitions of both the commercial and non-commercial versions of the warranty. However, even if included as "firmware" under the applicable clause, the warranty only applies to a contract product or item if that item is specifically "listed." The whole problem with embedded technology is that it presents a situation that is "outside the box" of typical IT. By definition, embedded technology is *embedded* (integrated) into some other item. Unless the "host" item is itself information technology, agencies may not consider the need for Year 2000 compliance when acquiring that item. Failure to consider the Y2K compliance needs of the item means the item will not be "listed" in the solicitation or contract; hence, any Year 2000 Warranty, if one is included in the contract, will not apply to the item containing the embedded technology.

Lastly, the operational boundaries of the exception language are not clearly circumscribed. As discussed above, the clause requires warranted IT to accurately process date/time data "to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it."[247] Presumably the purpose of this exceptionary language is to

---

[246] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.
[247] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

limit the IT contractor's liability for the non-compliant performance of other IT. However, contractors could interpret the language as follows: where the acquired IT *does not* interface with other IT, there is no requirement for the acquired technology to meet the performance standard. Focusing in on the portions of the clause at issue, the warranty reads as follows: "The contractor warrants that each . . . product . . . shall be able to accurately process date/time data . . . to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it."[248]

Under this interpretation, the performance requirement for the warranted IT is contingent upon it being operated in combination with other IT and even then, accurate date/time processing is required only when that other IT properly exchanges date data with the warranted IT. In short, the warranted IT must accurately process date/time data *only* when operated in combination with properly exchanging IT. When operated by itself or in combination with IT that improperly exchanges date data, the warranted IT need not meet the performance standard. Government agencies would likely argue that the phrase "to the extent" describes the range over which the standard of performance extends, establishing its scope and comprehensives,[249] rather than limiting its coverage to a single circumstance. Such an interpretation, an agency might argue, frustrates the purpose of the warranty and, as such, could not reasonably be considered a possible rendering of the clause. However, this interpretation is consistent with the warranty language and does prescribe a standard of performance for IT interoperability. More importantly, where the warranty language is ambiguous,

---

[248] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[249] See WILLIAM MORRIS, EDITOR, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (Houghton Mifflin 1976). Webster's New World Dictionary defines extent as "1) the space, amount or degree to which a thing extends; size; length; breadth 2) range or limit of anything; scope; coverage." VICTORIA NEUFELDT, EDITOR IN CHIEF, WEBSTER'S NEW WORLD DICTIONARY (Prentice Hall 3rd college ed. 1994).

B. Curtis

the ambiguity would be strictly construed against the government under the principle of *contra proferentem.*[250]

The "provided" exception language used in the original warranty clause lent itself more readily to this interpretation than the "to the extent" language: "The contractor warrants that each . . . product . . . shall be able to accurately process date data . . . provided that all listed or unlisted products (e.g. hardware, software, firmware) used in combination with such listed product properly exchange date data with it."[251] In the context of a warranty, the word "provided" serves as a stipulation: the warrantor agrees to meet the performance standard on the condition that interfaced IT properly exchanges date data.[252] Here again, where no such interface occurs, is there any obligation? In attempting to explain the meaning of the "provided" clause one source states that "[t]he word 'provided' is emphasized in the foregoing excerpt to demonstrate that the *basic requirement of Year 2000 compliance* contained in the GSA warranty *was expressly conditioned* on the ability of products other than the warranted IT product to exchange date data 'properly' with the warranted IT product."[253] If the basic compliance requirement is conditioned upon the ability of other IT products to successfully interface with it, then arguably where no interface takes place no standard of performance is warranted.[254] Obviously GSA did not intend IT contractors to warrant their products only when they were operated with other IT that properly exchanged date data, while

---

[250] *See, e.g.* Shirley Construction Corp., ASBCA No. 46670, 94-2 BCA, April 18, 1994.

[251] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[252] The American Heritage Dictionary of the English Language defines *provided* as "[o]n the condition; if" noting that "provided" is preferred where "a requirement is explicitly set forth," but that "[w]hen a mere condition or possibility is expressed *if* is proper." WILLIAM MORRIS, EDITOR, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (Houghton Mifflin 1976). To achieve the meaning probably desired by the warranty's drafters, the word "if" should have been used rather than "provided."

[253] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9, *emphasis added.*

[254] Kenney and Mason do not make this argument in their article. Nevertheless, the wording they chose to clarify the meaning of the "provided" language in the original GSA warranty is just as easily construed as limiting the performance obligation to instances of successful interoperability.

B. Curtis

bearing no obligation for the Year 2000 capability of their products when operated in stand-alone mode.[255]

Fortunately, the DAR Council has made it clear what that same exception language meant when used in the FAR clause. The DAR Council intended to limit the compliance requirement when the acquired IT is used in combination with other IT.[256] It does not want that limitation--intended to protect IT contractors from being responsible for the performance of other IT products--to nullify the performance requirement altogether. The "to the extent" language was added to the GSA Year 2000 Warranty clauses when they were revised to comport with the final FAR Year 2000 compliance provisions. While the DAR Council's intent behind the exception language is important, the plain language permits the nullifying interpretation and presents an issue that should be considered when using one of the warranty clauses.

IV. FAR YEAR 2000 COMPLIANCE REQUIREMENT

Because the Year 2000 problem stems from the decision in the early years of computer programming to store year date data using two digits rather than four, some consider the Year 2000 problem as an issue only for legacy systems. However, because storing year data with only two digits became a programming convention, even IT products currently used in manufacturing and available on the market today may have components or software that will be just as unreliable at processing Year 2000 dates as the "old" systems installed decades ago. In consideration of this reality, both the Chief Information Officers Council and the Interagency Group on the Year 2000

---

[255] Kenney and Mason recognize that under the language of the [original] GSA 'Year 2000 Warranty' clause, an IT vendor might attempt to argue that it had no Year 2000 compliance obligation at all, even with respect to its own products, simply because the IT products with which its products were required to interface were not Year 2000 compliant. They also conclude that "[t]his is clearly not the intent of the GSA warranty language." Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9.

[256] *See* Memorandum from Captain D.S. Parry, Director, Defense Acquisition Regulations Council, to Edward C. Loeb, Chairman, Civilian Agency Acquisition Council (June 13, 1997) (found in Case File 96-607 at the FAR Secretariat). This memorandum is discussed below in the section on the Final rule, FAR Year 2000 Compliance Requirement.

B. Curtis

determined that they needed to revise the FAR to insure the federal government would only acquire IT if that technology were capable of working properly in the Year 2000.[257] To implement that intention, the FAR Council[258] amended the FAR to provide "a uniform approach and definition for addressing the [Y]ear 2000 problem in the many unique information technology acquisitions that will occur between [January 1, 1997] and the [Y]ear 2000."[259]

A. INTERIM RULE

The Administrators of GSA and the National Aeronautics and Space Administration and the Secretary of Defense determined that there were urgent and compelling reasons to promulgate the interim rule before allowing the statutorily required[260] period for public comment.[261] The preamble to the interim rule indicates that the FAR Council was concerned that any delay in issuing an interim rule left federal agencies with the potential to procure additional non-compliant IT.[262] Such procurements, they explained, would needlessly consume even more government resources in the form of premature replacements or costly repairs to enable newly acquired non-compliant systems to properly process millennial dates.[263] The other potential result of acquiring additional non-compliant IT is the enlargement of the number of non-compliant government computers which will eventually malfunction or

---

[257] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, Jan 2, 1997.

[258] One segment of GSA employees operate the FAR Secretariat. *See* FAR 1.201-2. In this capacity, the staff not only performs the administrative procedures required to implement FAR changes, but often--as was true in the case of the Y2K compliance provisions--provides draft language to the CAA and DAR Councils to consider as they work towards amending the FAR.

[259] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, Jan 2, 1997.

[260] 41 USC § 418b, Public Law 98-577; see also 48 C.F.R. 1.501 (FAR 1.501). Section 418b(b) requires a period of not less than 30 days (counting from the date a proposed rule is published in the Federal Register) for public comment before a final rule may be issued. 41 USC § 418b(b). Section 418b(d) contains a waiver provision for situations where "urgent and compelling circumstances make compliance with such requirements impracticable." 41 USC § 418b(d).

[261] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 273-274, Jan 2, 1997. The interim rule included a request for comments which would be considered in formulating a final rule, calling for the submission of all comments on or before March 3, 1997. *Id.*

[262] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

[263] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

B. Curtis

fail when they encounter Year 2000 dates, [264] having neither been replaced nor corrected before they reached their "failure horizon."[265]

On January 2, 1997, the Civilian Agency Acquisition Council (CAAC or CAA Council) and the Defense Acquisition Regulations Council (DARC or DAR Council) published Federal Acquisition Circular 90-45, amending the FAR on an interim basis "to increase awareness of Year 2000 procurement issues and to ensure that solicitations and contracts address Year 2000 issues."[266] The interim rule addressed Year 2000 issues in two ways: first, it established a single, government-wide definition of "Year 2000 compliant."[267] Second, it created a requirement for government agencies who need IT to process dates beyond December 31, 1999 to acquire only Year 2000 compliant technology or technology which will be compliant by the time it is required to be so.[268] The compliance definition was based heavily upon the language crafted for GSA's recommended Year 2000 Warranty.

1. *"Year 2000 Compliant" Defined*

The interim rule added the following definition of "Year 2000 compliant" to the definitions found in FAR 39.002:

> Year 2000 compliant means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.[269]

---

[264] The preamble to FAC 90-45 did not discuss this possibility; nevertheless, the likelihood of this being another ramification of non-compliant IT acquisitions cannot be denied.

[265] A "failure horizon" is the date at which a particular agency or company, or a particular information technology system will begin to experience errors, failures or shut-downs due to its inability to properly process date data from the Year 2000 or beyond.

[266] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

[267] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997. The interim rule added a definition of "Year 2000 compliant" to the definitions found at FAR 39.002.

[268] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997. The interim rule renumbered FAR 39.106 to 39.107 and substituted a Year 2000 compliance requirement as FAR 39.106.

[269] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

B. Curtis

With this one definition, the FAR Councils[270] established a single standard for the entire federal government[271] to use when acquiring and upgrading the federal IT inventory.[272] In laymen's terms, the definition requires IT to do the following if it is to be considered "Year 2000 compliant." First, the IT must accurately process date/time data regardless of whether the data expresses a twentieth century (1900s) or twenty-first century (2000s) date and/or time. The term "accurately processes" is not defined, but is elucidated by the use of several non-exclusive examples: calculating, comparing, and sequencing. A common example of a software application that processes dates by calculating would be one that computes interest, determining the interest period by subtracting the loan origination date from the current date, then multiplying the result with the applicable interest rate to arrive at the amount of interest. Date comparing is used commonly in applications designed to take a particular action on a specified date. A microprocessor in an automobile compares the current date to the "next-maintenance-date" programmed into the processor by the last maintenance technician to determine if the proper time interval between regular maintenance procedures has elapsed. If so, the "next-maintenance-date" has been reached, and a "maintenance

---

[270] The term "FAR Councils" is used in this paper to denote the DAR and CAA Councils, and not *the* "FAR Council" composed of the Administrator for Federal Procurement Policy, the Secretary of the Defense, the Administrator of National Aeronautics and Space Administration, and the Administrator of General Services. The FAR Council has overall authority to prepare, issue and maintain the FAR and to prescribe the FAR System. *See* 41 USC 421 and FAR 1.103. The DAR and CAA Councils (the FAR Councils) each have cognizance over specific portions of the FAR, taking the primary responsibility for drafting necessary revisions, and then, through coordination, jointly approving and publishing those changes. *See* FAR 1.201-1.

[271] This grand statement is made with an understanding that the United States Postal System and several smaller segments of the federal government are not subject to the FAR. Nonetheless, contracting functions for these exempt agencies are still able to reference FAR standards in their contracts and should be addressing Y2K issues in their contracts.

[272] The GSA heralded the FAR change, stating that "[w]hile seemingly a minor issue, the importance of a standard definition cannot be over emphasized. . . . Its development represents a major breakthrough and is a vital first step in developing contractual compliance language." GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

B. Curtis

required" message is displayed on the car's dashboard.[273] Sequencing is a process which might be used by any date-sorting software routine, such as when a computer in a hospital's records section automatically organizes a patient's computerized treatment records based upon the date when the patient received the medical care.[274] Whatever method is used--calculating, comparing, sequencing, or even some other--to process date/time data, for the IT to be considered "Year 2000 compliant" the process will have to yield accurate results.

Second, the rule describes the accurate date/time processing requirement as applicable to both "the twentieth and twenty-first centuries" and "the years 1999 and 2000."[275] Dual descriptors were probably used to ensure the widest possible application and to close any potential linguistic loopholes in applying the compliance standard. Technically speaking, the twentieth century will terminate on December 31, 2000 and the twenty-first century will begin on January 1, 2001. As mentioned above,[276] many will mistakenly celebrate the new century, and the new millennium, with the arrival of January 1, 2000. It is possible the phrase "twentieth and twenty-first centuries" was used to indicate that "compliant" IT will be able to accurately process dates from whenever the IT was purchased[277] through December 31, 2100--the literal end of the twenty-first century. However, it is more likely that the phrase "twentieth and twenty-first centuries" was used to address the popular (though imprecise) understanding of those terms as referring to the years 1999 and 2000. The original version of the GSA

---

[273] A similar "compare" function occurs at the video rental store when the computer compares the expiration date on a driver's license to the current date to insure that the person attempting to open a rental account is using a valid driver's license.

[274] The same sort of sequencing occurs when a credit card company's computer prepares a monthly billing report for an individual debtor, taking all of the credit transactions which have arrived at various intervals throughout the billing period, and not necessarily in the order in which the credit was used, and chronologically arranges the charges on the billing report.

[275] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

[276] See the section on Terminology above in Chapter II.

[277] The "twentieth century stretches from January 1, 1901 through December 31, 2000 and the twenty-first century begins January 1, 2001 and ends on December 31, 2100. Obviously even this coverage is limited in that information technology might be required to process dates beyond December 31, 2100.

B. Curtis

warranty did not include the more specific language "and the years 1999 and 2000."[278] The numbers "1999 and 2000" were likely included in the FAR language to cover those who might otherwise suggest that they understood the "twentieth and twenty-first centuries" requirement in its technically precise sense, calling for accurate processing between the pivotal century-bounding years 2000 and 2001, rather than 1999 and 2000.[279]

Third, the rule tacks on the phrase "and leap year calculations," without any specific reference or explanation. This bare reference also functions as a "loophole closer," putting all on notice that leap years must be taken into account wherever they may fall. Although one might have expected a more specific reference, such as "leap year, 2000" or "February 29, 2000," it is possible that those framing the rule were not altogether certain whether 2000 would be a leap year. In 1997 people were still arguing about whether, in fact, the Year 2000 would be a leap year.[280] Considering how few people are aware of the leap year rule dealing with years divisible by 100 or 400, the confusion is understandable. To be "Year 2000 compliant," IT will have to take February 29, 2000 into account when performing date/time processing and, arguably, accurately process date/time data for every other leap year as well.

Fourth, there is an additional hurdle for IT to leap before attaining "Year 2000 compliant" status: the IT must be able to perform its accurate date/time date processing in combination with other IT if that other IT properly exchanges date/time data with it. This mandate for interoperability was stated separately from the foregoing

---

[278] See *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[279] One commenter on the interim rule assumed the mismatched references to "the twentieth and twenty-first centuries" and "the years 1999 and 2000" were unintentional. Comments from Richard Sturgis, Contracting Officer, U.S. Army Communications-Electronics Command, Acquisition Center--Washington Operations Office, March 3, 1997, found in Case File 96-607 at the FAR Secretariat. Technically speaking, because the "twentieth century" includes the Year 1999 and the Year 2000, and the language "from, into, and between" was included, the term "twentieth century" would have covered the Year 2000 Problem, whether applied in its technical or popular sense.

[280] Ashley Dunn, *Y2K Bug: Problem for the Ages*, WISCONSIN ST. J., at 1C, August 21, 1998.

B. Curtis

requirements, set off as an additional sentence. The division of the compliance definition into two sentences created a potential interpretation problem, setting the stage for an interpretation that the two sentences create independent compliance obligations, each of which had to be met in order to attain Year 2000 compliance.

The second sentence in the definition begins with the word "furthermore." "*Furthermore*, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it."[281] This sentence would normally be interpreted as an indication that a contractor's product must meet both the requirements set out before the word "furthermore" and also the requirements that follow in order to be "Year 2000 compliant." Viewing the two sentences as independent compliance obligations could lead to the conclusion that a contractor's product would only be considered Year 2000 compliant if it correctly processed date/time data 1) when used in combination with other IT which properly exchanged date/time data with it (the "furthermore" sentence) and 2) if used individually or even in combination with IT that did not properly exchange date/time data with it (the first sentence). It was this possible interpretation that proved most alarming to the IT industry.[282] While this interpretation might not have been the most likely or straightforward rendering of these two sentences, IT contractors had to consider this interpretation as they struggled to understand why the interim FAR definition of compliance differed from the construction of the compliance definition used in the GSA Year 2000 Warranty clause.[283]

The initial version of the GSA Year 2000 Warranty clause stated:

---

[281] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997, *emphasis added*.
[282] Robert J. Kenney, Jr. and Michael , *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9.
[283] *See* Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9.

B. Curtis

The contractor warrants that each hardware, software, and firmware product delivered under this contract and listed below shall be able to accurately process date data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, including leap year calculations, when used in accordance with the product documentation provided by the contractor, *provided* that all listed or unlisted products (e.g. hardware, software, firmware) used in combination with such listed product properly exchange date data with it.[284]

The original GSA warranty clause used the term "provided," but the interim FAR clause used the term "furthermore." Under the terms of the original GSA warranty clause, the requirement for an IT item to accurately process date data, when used in combination with other IT, was expressly conditioned upon the other IT properly exchanging date data with the warranted item. Without any preambulary explanation for the FAR clause's change in the construction of the definition, industry representatives were left to imagine why the conditioned interoperability requirement in the GSA warranty had arguably become independent compliance requirements in the FAR's compliance definition. The FAR definition could be seen as requiring IT to interoperate effectively with non-compliant IT and, "furthermore," with compliant IT, so as to accurately process date/time data whether operating independently or in combination with other (compliant or non-compliant) IT. There was nothing unusual in demanding IT products to perform accurate date-processing, both when operating independently and when connected to other compliant IT. However, a requirement to interface with non-compliant IT and still process date data accurately was the type of exorbitant performance requirement IT contractors would have expected the newly crafted standard definition to preclude.

Viewing the first sentence of the FAR definition from the perspective of independent compliance requirements, an IT contractor would face the risk of having its otherwise compliant product being deemed non-compliant because of problems that

---

[284] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 GOV'T CONTRACTOR (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996, *emphasis added.*

B. Curtis

occurred when it was required to interface with IT products the government was purchasing from other IT contractors, or when the government's legacy systems were interfaced with the newly acquired product. Whether the problem stemmed from the "other" IT's noncompliance or from its inability to properly exchange date/time data with the acquired IT, the acquired IT would be considered "non-compliant" whenever it failed to properly process date/time data, regardless of the cause. Asking a contractor to guarantee the Year 2000 compliance of government systems, other contractors' products, or any system that would ever be interfaced with the acquired IT--in addition to guaranteeing the compliance of its own product--would be asking the contractor to guarantee integration scenarios it could not even reasonably foresee or predict.

Although the circular introducing the FAR definition made no explanation for the switch, the term "provided" used in the original GSA warranty was probably changed to "furthermore" to prevent an interpretation that the acquired IT was required to accurately process date data *only* when interfaced with other compliant IT. Such an interpretation, flowing from the "provided" language would render the compliance requirement applicable to a single situation: where the acquired IT was interfaced with similarly compliant IT. Information technology contractors should certainly be prepared to warrant that their products will accurately process date data both when used independently *and* when used with similarly compliant IT. The change from "provided" to "furthermore" is more reasonably interpreted as an attempt to insure the IT is required to process accurately when operated individually, rather than as an attempt to force IT contractors to guarantee their products' processing capabilities even when operated with non-complaint IT.[285]

---

[285] *See* Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9. This interpretation is discussed above in the section on Issues under the GSA's Year 2000 Warranty.

B. Curtis

This troublesome interpretation was obviously unintended,[286] as was demonstrated by the final rule revisions.[287] When published, the final "Year 2000 compliant" definition had been revised, replacing "furthermore" with language that clearly limits the IT contractor's obligations to its own products. Rather than requiring that IT products properly interface with other equipment "provided" that the other equipment properly exchange date data with it, the final version states that the delivered IT will properly interoperate "to the extent" that the interfacing IT properly exchanges date data with it.[288] Those who may have been disturbed by the interim definition's possible interpretation were undoubtedly pleased with the new "to the extent" exemption language which removed all the onerous possibilities the IT contractors may have envisioned. GSA stated that the "change [in the final rule] did not impact the meaning or intent of the definition,"[289] indicating their viewpoint that the interim version of the FAR definition was more a result of the difficulty attending the precise crafting of a seamless definition than the expression of an intention to levy unreasonable compliance obligations upon IT contractors.

---

[286] *See* Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9 ("It appears likely, at least in retrospect, that the feared implication of the interim rule on this point was not deliberate.")

[287] In fact, in preparing language for the interim rule, the FAR Information Technology Committee had proposed to include warranty clauses almost identical to the GSA Year 2000 Warranty clauses in FAR 52.239. Those clauses differed from the FAR 39.002 definition of Year 2000 compliant published in the interim rule in that they 1) used the "provided" language rather than "furthermore," 2) retained the proviso that the product was "used in accordance with the product documentation provided by the contractor," and 3) did not use the more accurate year references 1999 and 2000. Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (October 28, 1996) (found in Case File 96-607 at the FAR Secretariat).

[288] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

[289] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 1.4, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. The changes made were characterized as only "a minor sentence structure revision to the FAR 39.002, Year 2000 compliant definition." *Id.*

B. Curtis

2. *Compliance Required*

The interim rule created the following Year 2000 compliance requirement, to be inserted into the FAR at section 39.106:

> When acquiring information technology that will be required to perform date/time processing involving dates subsequent to December 31, 1999, agencies shall ensure that solicitations and contracts--
> (a)(1) Require the information technology to be Year 2000 compliant; or
> (2) Require that non-compliant information technology be upgraded to be Year 2000 compliant prior to the earlier of
> (i) the earliest date on which the information technology may be required to perform date/time processing involving dates later than December 31, 1999, or
> (ii) December 31, 1999; and
> (b) As appropriate, describe existing information technology that will be used with the information technology to be acquired and identify whether the existing information technology is Year 2000 compliant.[290]

Just as the interim rule established a single, government-wide standard for defining Year 2000 compliance, it also established a government-wide requirement applicable when federal agencies acquire IT. Without this mandate, the definition merely provided an easily referenced standard for government IT acquisitions. The requirement portion of the rule provided the force necessary to implement the government's goal of stemming the tide of non-compliant equipment flowing into the federal IT inventory.

The new rule required agencies to include certain requirements in their solicitations and contracts for IT, but only if the IT were going to be used to perform date/time processing involving dates beyond December 31, 1999. If an agency needed IT for an application that did not require the processing of date or time data, or if the data to be processed were all prior to January 1, 2000, the agency would not need to concern itself with the requirements of this provision. Where the rule applied, the agency could either require the contractor to provide only Year 2000 compliant IT or the agency could allow the contractor to provide non-compliant IT initially and then bring the IT into Year 2000 compliance before the IT was required to process millennial dates. The rule also instructs agencies to describe any IT that will interface with the

---

[290] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

B. Curtis

acquired IT, advising the contractor as to that IT's compliance status. While these two FAR clauses force federal agencies to address Year 2000 compliance when procuring most IT, they do not spell out the ramifications for the contractor who delivers or develops non-compliant IT products under contracts which clearly required Y2K compliance. In describing the implementation of this requirement, the DAR Council advised that standard contract clauses provide adequate means for addressing non-compliance.[291]

The GSA Year 2000 Warranty clause is voluntary. The FAR Year 2000 compliance rule is mandatory and agencies may deviate from the requirement only through the FAR's formal deviation process.[292] If an agency desires to procure IT that neither is nor will be Year 2000 compliant--as that term is defined in the FAR 39.002--by the deadline established in FAR 39.106, the agency head or his designee may authorize such deviation, but only after documenting the justification and approval for the deviation in the contract file.[293] A situation could hypothetically exist where an agency determined that the best IT proposed to meet its needs was not currently able to process date/time data in compliance with FAR 39.002 nor would upgrades reasonably be available to provide this capability by December 31, 1999. The requirement in FAR 39.106 assumes that all IT that will process date/time data needs to be able to do so by December 31, 1999. If a particular application did not require the IT to process millennial dates until some time after January 1, 2000, then the proposed IT might still be the most appropriate choice for the agency, assuming it would be made Year 2000 compliant before it would ever actually be required to process millennial dates. This "individual deviation" is effective only for one contracting action.[294] The FAR also provides for agency heads to approve "class deviations," which would be

---

[291] DAR Council, "Explanation of FAR Language," posted at
http://www.govexec.com/dailyfed/0298/020598bt.htm, site visited on September 25, 1998.
[292] See generally 48 C.F.R. Subpart 1.4--Deviations from the FAR.
[293] FAR 1.403.
[294] FAR 1.403.

B. Curtis

effective for multiple contracting actions, but only after consulting with the applicable FAR Council.[295]   Considering the seriousness of the compliance issue and the increasing congressional and public scrutiny of Y2K problems in government, it is highly unlikely that many agency heads or either FAR Council would be inclined to look with favor on requests to deviate from the FAR's Year 2000 compliance requirement.

B. FINAL RULE

During the comment period, the FAR Secretariat received twenty comments from five respondents.[296] After considering each of the comments, the FAR Councils revised the definition provided in the interim rule and issued a final rule on August 22, 1997. The GSA heralded the rule: "This provides agencies a standard, Government and industry accepted definition of Year 2000 compliant products,"[297] noting that industry had played a role in the language of the final FAR definition, much as it had in negotiating the GSA Year 2000 Warranty clauses.

1. *Revised Language*

The Federal Acquisition Circular (FAC) publishing the final rule, FAC 97-01, states that the revision of the "Year 2000 compliant" definition was made "to better convey the intent of the definition."[298]   The revisions were not made because of a change in the government's goals, but because the public comments and internal decision-making discussions had made it apparent that the language used in the original definition had not clearly conveyed the compliance requirements envisioned by the DAR and CAA Councils.[299] The final rule defined Year 2000 compliant as follows:

---

[295] FAR 1.403. Here the term obviously refers to whichever Council (CAA or DAR) has primary responsibility for the particular area at issue.

[296] FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44830, Aug 22, 1997.

[297] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[298] FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44802, 44830, Aug 22, 1997.

[299] "The final rule differs from the interim rule in that it makes clarifying revisions to the definition of "Year 2000 compliant" at FAR 39.002." FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44802, 44833, Aug 22, 1997.

B. Curtis

Year 2000 compliant, as used in this part, means, with respect to information technology, that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.[300]

The interim rule stated that "Year 2000 compliant means information technology that accurately processes," and the final rule stated that "Year 2000 compliant, as used in this part, means, with respect to information technology, that the information technology accurately processes." The former version focuses on information technology as though only information technology can be Year 2000 compliant or non-compliant, apparently dismissing the possibility that other supply items might pose Year 2000 problems. The final rule takes a more specific view, limiting itself to the compliance of IT and acknowledging, at least tacitly, that other supply items may present Year 2000 compliance issues as well.

With the CAA Council's concurrence, the DAR Council replaced the "furthermore" language with "to the extent" language. The DAR Council found the exception language published in the interim rule as troubling as industry may have, but for the opposite reason. "We have revised the second half of the [interim] definition to clarify that the improper exchange of data is a limited exception to the requirement for accurate processing of date/time data, rather than a condition which nullifies the entire Year 2000 compliance requirement."[301] The DAR Council apparently found the "furthermore" exception to be susceptible of the interpretation that the compliance standard applied *only* when the acquired IT was operated with "properly-exchanging" IT. This same "nullifying" interpretation problem existed with the "provided" language

---

[300] FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44830, Aug 22, 1997.

[301] Memorandum from Captain D.S. Parry, Director, Defense Acquisition Regulations Council, to Edward C. Loeb, Chairman, Civilian Agency Acquisition Council (June 13, 1997) (found in Case File 96-607 at the FAR Secretariat).

B. Curtis

used in the original GSA Year 2000 Warranty clauses.[302]   In fact, the "to the extent" language selected by the DAR Council is actually more susceptible of being rendered as "nullifying" the compliance requirement than the "furthermore" language it replaced.[303]   If disputes over the performance standard arise between agencies and IT contractors, the agency may be forced to argue beyond the plain language used in the compliance definition[304] and point to the DAR Council's comments in the rule's Case File. The goal was to protect IT contractors from warranting the performance of other IT which was used in combination with the contractor's IT. The comments demonstrate that the DAR Council explicitly sought to avoid any interpretation of the compliance definition which nullified the compliance requirement.[305]

2. *Retained Language*

The compliance requirement was not changed at all in the final rule, but remained as it had been published in the interim rule.   The basic standard of performance required in the Year 2000 compliant definition also remained the same in the final rule: compliant IT "accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations."[306] None of the commenters discussed the inclusion of "leap year" in the definition, so the term remained, albeit unclarified.

---

[302] The section above regarding the "Year 2000 compliant" definition used in the interim rule discusses this interpretation of the "provided" language in the original GSA Year 2000 Warranty clauses.

[303] The section above discussing "issues" to be considered under the GSA Year 2000 Warranty clauses.

[304] This assumes that the agency included the Year 2000 Compliant definition from FAR 39.002 in the contract, either expressly or by reference, rather than attempting to achieve compliance through agency-developed specifications. Such specifications are appropriate in some situations and doubtlessly are required in others; however, agencies must use great care when drafting such specifications and would probably do well to include the FAR 39.002 definition as a reference point and then add specifications as necessary.

[305] *See* Memorandum from Captain D.S. Parry, Director, Defense Acquisition Regulations Council, to Edward C. Loeb, Chairman, Civilian Agency Acquisition Council (June 13, 1997) (found in Case File 96-607 at the FAR Secretariat).

[306] FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44830, Aug 22, 1997.

B. Curtis

A government contracting officer commented, pointing out that the references to "the twentieth and twenty-first centuries, and the years 1999 and 2000" were not consistent.[307] The FAR Information Technology Committee's response to the comment in its report was that "[t]he definition clearly applies to date/time data changes between the two centuries. Therefore, no change is necessary."[308] The Chair of the Government Contracts Section of the Federal Bar Association raised the same issue of ambiguity, focusing on the demands implicit in requiring compliance for entire centuries rather than just the date change between the years 1999 and 2000.[309] He suggested that If an IT product must be able to accurately process dates "from now through 2099," products which retain "the two-digit Real Time Clock found in most computers" will not be able to use a simple windowing algorithm to address the Year 2000 Problem.[310] Once again, the Committee Report's answer to this concern merely concluded that "[t]here is no

[307] "[T]he proposed language unintentionally, but literally, applies to the change 'from, into, and between' 2000 and 2001, not 1999 and 2000, because both 1999 and 2000 are in the twentieth century." Comments from Richard Sturgis, Contracting Officer, U.S. Army Communications-Electronics Command, Acquisition Center--Washington Operations Office, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat).

[308] Memorandum from Edward C. Loeb, Chairman, Civilian Agency Acquisition Council, to Captain D.S. Parry, Director, Defense Acquisition Regulations Council (April 9, 1997) (found in Case File 96-607 at the FAR Secretariat), at p 6. The Committee's response does not make it clear that the Committee understood the point the commenter was attempting to communicate. The focus of the Year 2000 Problem is the date change from the Year 1999 to 2000. As the commenter pointed out, those two years are in the *same* century, the twentieth, rather than in the twentieth and twenty-first centuries. The Committee's response would make sense if the definition were intended to apply to two distinct situations: 1) twentieth (January 1, 1901 to December 31, 2000) and twenty-first century (January 1, 2001 to December 31, 2100) dates, *and* 2) the Years 1999 (ending December 31, 1999) and 2000 (beginning January 1, 2000). However, the Committee's response emphasizes the phrase "*and the years 1999 and 2000*" and then concludes that "[t]he definition clearly applies to date/time changes between the two centuries." *Id.*

[309] Comments from Alex D. Tomaszczuk, Chair, Government Contracts Section, Federal Bar Association, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat). "One interpretation of this language is that Year 2000 compliant equipment must accurately display the current date throughout the rest of this century and the entire next century; that is, a capability to accurately process date/time data from now through 2099." While the commenter properly perceives the potential extent of the terms--covering the entire twenty-first century rather than merely the boundary years 1999 and 2000--the commenter makes the same technical error that others make by stating that a century ends with the "99" year rather than the "00" year. *Id.*

[310] Comments from Alex D. Tomaszczuk, Chair, Government Contracts Section, Federal Bar Association, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat).

B. Curtis

need to change the FAR language because there is no ambiguity in that definition."[311] So, whether *in spite of* the apparently disparate references to the same years, or *because* both the 1999 to 2000 year change *and* the two named centuries were intended to be included in the definition, this portion of the definition was retained without change.

C. IMPLEMENTATION

Without a doubt, the addition of the Year 2000 compliance provisions to the FAR was a great step for the federal government towards keeping its Y2K problems from growing through continuing, albeit inadvertent, non-compliant IT procurements. In describing the FAR's new Year 2000 compliant definition GSA stated that "[i]ts development represents a major breakthrough and is a vital *first step* in developing contractual compliance language."[312] While praising the regulatory definition, GSA recognized it as the starting point from which contracting authorities would need to build more precise technical specifications. "Carefully crafted by Government, with significant input from industry, the new FAR definition serves as a *baseline* for agreement on what constitutes Year 2000 compliance."[313] Standing alone, the FAR definition will not effectively address every set of government requirements for IT.

Government agencies retain a large measure of flexibility in implementing the compliance requirement as the rule does not mandate any particular method for requiring Year 2000 compliance in solicitations and contracts. Agencies might implement the compliance requirement by including the appropriate GSA Year 2000

---

[311] Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997) (found in Case File 96-607 at the FAR Secretariat), at p 7.

[312] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998, *emphasis added.*

[313] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

B. Curtis

Warranty clause in their contracts. In the language accompanying the warranty clauses, GSA claims that its warranty is a sufficient means of achieving the compliance required by the FAR provisions.[314] However, in its guidance on applying and implementing the FAR definitions of Year 2000 compliant, GSA has taken a somewhat different position on the sufficiency of its warranty clauses:

> Even with its advantages, the warranty provisions may not in all cases meet an agency's requirement. In some cases the nature and complexity of the system may warrant the development of specialized solicitation/contract language. Highly complex software development projects of development efforts for critical systems may warrant a higher degree of Year 2000 coverage than that provided by a warranty provision.[315]

While considering the comments from industry on the interim FAR Y2K provisions, the FAR Information Technology Committee decided that the GSA Year 2000 Warranty clauses should be included in the FAR on an interim basis, providing an opportunity for public comment on those portions of the rule.[316] The Committee also concluded that contracting officers should have several options for implementing the compliance requirement in contract documents. "The committee report makes it clear that the committee intended for specifications to be used as an alternative to the warranty clauses or in addition to the warranty clauses."[317] As the Committee saw it, an

---

[314] http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998. "NOTE: COMPLIANCE WITH THE AUGUST 22, 1997 FINAL FAR RULE ON YEAR 2000 COMPLIANCE CAN BE ACHIEVED WITH THE REVISED AUGUST 22, 1997 RECOMMENDED YEAR 2000 CONTRACT LANGUAGE DEVELOPED FOR THE CIO COUNCIL SUB-COMMITTEE ON THE YEAR 2000." *Id.*

[315] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.2, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. In its conclusion, the paper states that the "warranty provisions are considered particularly applicable to COTS products and non critical development/integration efforts." *Id.* at section 3.

[316] *See* Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997) (found in Case File 96-607 at the FAR Secretariat).

[317] Memorandum from Edward C. Loeb, Chairman, Civilian Agency Acquisition Council , to Captain D.S. Parry, Director, Defense Acquisition Regulations Council (April 9, 1997) (found in Case File 96-607 at the FAR Secretariat). In fact, the FAR changes proposed by the FAR Information Technology Committee were that where "[a]n agency [was] acquiring information technology that will be required to perform date/time processing involving dates subsequent to December 31, 1999, [the agency] may" include 1) one of the warranty clauses, 2) contract specifications to achieve compliance, or 3) no Year 2000 compliance

agency might use contract specifications, the GSA warranty, or both to achieve the Year 2000 compliance requirement in an IT contract.

The warranty clauses were not published as part of the final rule, largely because the DAR Council determined that they would have been counterproductive. That same view is expressed in the DAR Council's position on implementation, which discourages the use of warranties as a means of achieving the required compliance.[318] The Council notes that adding warranties--whether GSA's or some other Year 2000 warranty--may tend to drive up the cost of a contract and, therefore, discourages that method.[319] Another means of implementing the compliance requirement is to build those requirements into the specifications included in all solicitations for IT. The DAR Council espouses this method of implementation, explaining that "[i]f the Year 2000 compliant requirement is properly specified, then the Government has existing contractual remedies if the contractor fails to deliver a compliant system."[320]

It is important to note the difference in acquisition perspectives between GSA and the DoD. GSA acquisitions more commonly fall within the arena of commercially available supply items and the DoD, although increasingly buying commercial items where those products will meet its needs, often has supply requirements which can be

---

provisions. Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997) (found in Case File 96-607 at the FAR Secretariat). It was the CAA Council that envisioned the additional option: "As an alternative to or in conjunction with using one of the [warranty] clauses prescribed [by the FAR], the Government may address the need for Year 2000 compliant information technology in the contract specification." Memorandum from Edward C. Loeb, Chairman, Civilian Agency Acquisition Council , to Captain D.S. Parry, Director, Defense Acquisition Regulations Council (April 9, 1997) (found in Case File 96-607 at the FAR Secretariat).
[318] DAR Council, "Explanation of FAR Language," posted at http://www.govexec.com/dailyfed/0298/020598bt.htm (September 25, 1998).
[319] "We discourage the use of warranties to avoid the possibility of paying for Year 2000 compliance twice ([o]nce when we price the requirement and once again when the contractor charges us for the warranty)." DAR Council, "Explanation of FAR Language," posted at http://www.govexec.com/dailyfed/0298/020598bt.htm (September 25, 1998).
[320] DAR Council, "Explanation of FAR Language," posted at http://www.govexec.com/dailyfed/0298/020598bt.htm, site visited on September 25, 1998. The DAR Council concludes that the key to protecting the government's interests is a clear specification of the compliance requirements rather than the inclusion of an additional warranty.

B. Curtis

met only through non-commercial item contracts. When the Chief Information Officer (CIO) Council tasked GSA with developing a Year 2000 Warranty, it specifically targeted commercial off-the-shelf (COTS) purchases, and specifically COTS information technology.[321] The GSA Year 2000 Warranty clause makes a great deal of sense when agencies are purchasing commercial supply items, and Year 2000 specifications make equally good sense when the agencies are purchasing non-commercial supply items. From the obverse perspective, it would make little sense to attempt to achieve Year 2000 compliance in COTS contracts through the use of specifications. The two concepts are antithetical. The government purchases commercial products specifically because its needs can be met by something that is already available in the marketplace. The agency does not need to draft detailed specifications describing the product it requires.

GSA actually suggested that the FAR's Year 2000 compliance requirements could be included in solicitations and contracts through either method: "Require the offerors/contractors to certify compliance and warrant their products" or "draft unique Year 2000 specification/statement of work (SOW) compliance language."[322] The Air Force provides an example of this method of implementation in its most recent procurement for the next generation of F-16 fighter aircraft. The Air Force has included the FAR's Year 2000 compliance requirement in its statement of work.[323] Some have questioned whether specifying Year 2000 compliance requirements beyond those

---

[321] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998). John Cornell, working along with Cynthia Warner and Larry Wolfe, was the principle author of the GSA Year 2000 Warranty clauses and the FAR clauses that were distributed to and modified by the FAR Councils.

[322] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.4, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[323] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998). Cornell, working with Cynthia Warner and Larry Wolf, was the principle author of the GSA Year 2000 Warranty clauses and the FAR Year 2000 compliance provisions, as they were provided to the FAR Councils.

B. Curtis

contained in FAR 39.002 would amount to a deviation from the FAR rules.[324] Clearly GSA did not think so when providing its implementation guidance.[325]

GSA's suggestion that contractors be required to warrant and certify their products Year 2000 compliance would run afoul of the FAR restriction on creating any new certifications.[326] In fact, the restriction on creating new contractor certification requirements flows from the National Defense Authorization Act for Fiscal Year 1996, now known as the Clinger-Cohen Act.[327] That same statute contained the Information Technology Management Reform Act which is discussed below. The Clinger-Cohen Act's provisions dealing with contractor certification requirements made it crystal clear that such requirements are not only disfavored, but will only be permitted following an approval process which includes a written justification submitted by the FAR Council and approved by the Administrator for Federal Procurement Policy.[328]

On its face the FAR 39.106 purports to regulate IT procurements only prospectively: "When acquiring information technology . . . , agencies shall ensure that solicitations and contracts--(a)(1) Require the information technology to be Year 2000

---

[324] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998), at 8. Kenney and Mason state that "[i]t is unclear whether an attempt by an agency to refine or augment the FAR definition of 'Year 2000 compliant' would be considered a deviation." *Id.* Discussing a scenario where the government specifies that the IT provided must employ a four-digit year date field, Kenney and Mason conclude that the vendor whose product uses a two-digit windowing solution could argue that a deviation was required and "would have the better argument, [although] the question has not yet been resolved." *Id.*

[325] See GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.4, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[326] FAR 1.107.

[327] Clinger-Cohen Act, 1996, Pub. L. No. 104-106, §4301, 110 Stat. 186, 657 (1996).

[328] Clinger-Cohen Act, 1996, Pub. L. No. 104-106, §4301, 110 Stat. 186, 657 (1996), codified at 41 U.S.C.d425. The pertinent provisions required the Administrator for Federal Procurement Policy to issue a proposal to remove all contractor/offeror certification requirements from the FAR unless specifically imposed by statute or the Administrator has approved the FAR Council's written justification of the requirement as the least burdensome means of achieving regulatory compliance. Secondly, no contractor/offeror certification requirement may be added to the FAR unless specifically imposed by statute or the Administrator for Federal Procurement Policy approves the FAR Council's written justification therefore. Finally, government agencies are prohibited from construing statutes as requiring contractor/offeror certifications unless the statute specifically mandates certification. The statute places similar restrictions on executive agencies regarding certification requirements in agency supplements. *Id.*

B. Curtis

compliant; or (2) Require that non-compliant information technology be upgraded to be Year 2000 compliant . . . ."[329] However, in the conclusion to its August 1997 explanation of the new FAR provisions, GSA stated that this clause "require[s] agencies to acquire Year 2000 compliant products both for new acquisitions and deliveries under existing contracts if they will be used to process date information from December 31, 1999, or later."[330] The DAR Council clearly anticipates that the FAR's compliance standards will be added to ongoing IT contracts: "If [the procurement] is an old contract, the contract should be modified to require Year 2000 compliance and the contractor should be appropriately compensated."[331] Regardless of which interpretation of FAR 39.106 is correct, the question was rendered moot by the enactment of the Treasury, Postal Service, and General Government Appropriations Act, 1998, which prohibits the use of funds appropriated in *any* Act "to acquire information technologies which do not comply with [FAR P]art 39.106."[332]

D. REMAINING ISSUES

1. *Embedded IT Systems*

In addressing Year 2000 compliance, neither of the new FAR sections include any reference to "embedded" IT. Rather, FAR 39.002 defines Year 2000 compliance in terms of "information technology"[333] and FAR 39.106 only restricts acquisitions of certain "information technology."[334] The definition of information technology is found in FAR 2.101 and expressly excludes embedded IT unless it is integrated into some article

---

[329] FAR 39.002.
[330] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.
[331] DAR Council, "Explanation of FAR Language," posted at http://www.govexec.com/dailyfed/0298/020598bt.htm, site visited on September 25, 1998.
[332] Treasury, Postal Service, and General Government Appropriations Act, 1998, Pub. L. No. 105-61, §631, 111 Stat. 1272, 1315 (1997). This section of the Act and the limited waiver provision are discussed below in Chapter VI.
[333] FAR 39.002.
[334] FAR 39.106.

B. Curtis

which independently qualifies as IT.[335] This exclusion is explained and explored in much greater detail below.

2. *Technical Solution Not Specified*

Just as with the GSA Year 2000 Warranty clauses, the Year 2000 compliant definition was not expressed in terms of a single technical solution, nor did the compliance requirement mandate any particular method of achieving compliance. GSA's implementation guide noted that a particular contract might achieve Y2K compliance by "specifying the actual date/time programming convention to follow in the development process,"[336] but the FAR Information Technology Committee made it clear that "[a]gencies may implement [the compliance] requirement in various ways."[337] The rule also instructs agencies to describe any IT that will interface with the acquired IT, advising the contractor as to that IT's compliance status. There is no guidance as to what exactly the contractor should be told. Presumably those on the agency's acquisition team will have sufficient technical background to know what information will be important for the contractor to know so that the acquired items will be able to properly interface when integrated with the agency's other IT. Sufficient contractor-agency communication, both before the solicitation and after contract award will insure that the products acquired employ a Y2K technical solution that is compatible with other agency IT.

The compliance standard in both the GSA warranty clauses and the FAR definition include an exception: the IT must accurately process date/time data at the

---

[335] FAR 2.101

[336] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.2, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[337] Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997) (found in Case File 96-607 at the FAR Secretariat), at p 7. "[T]he definition is not intended to tell agencies 'how' to achieve compliance nor to promote any one method or algorithm of patching older equipment." *Id.*

B. Curtis

prescribed times, "to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it."[338]

The initial version of the "Year 2000 compliant" definition was adjusted to meet industry concerns about one contractor becoming responsible for the compliance of equipment provided by other contractors. Hence the qualifier was added so that the procured IT need only process date/time data accurately with interfaced IT if the two successfully trade date data. Even though this qualifier was intended to ensure that a contractor was not held responsible for the ability of other IT to properly process and exchange date/time data, the qualifying language allows for unnecessary interoperability problems between systems that would defeat the purpose of specifying that only compliant IT be procured. Two contractors might reasonably select non-compatible methods of date/time data handling, each of which is a completely viable and acceptable method of addressing the date problem and yields an IT product which fully comports with the compliance definition. In spite of the fact that the two IT products could function properly working in a "stand-alone" mode, independent of interaction with each other, the non-compatible compliance methodologies would prevent the two products from being able to properly exchange information. Under the FAR's language, each vendor would be able to claim conformance with the requirement, pointing out that their system's failure to accurately process the data resulted from the inability of the other contractor's IT to properly exchange data. For example, the contractor whose system achieves compliance via a windowing technique will claim that the other contractor should likewise have selected the windowing solution, rather than implementing a four-digit date field. Therefore, although the interoperability language in the Year 2000 compliance definition was intended to protect

---

[338] The same language is found in the FAR Year 2000 Compliant definition, FAR 39.002, and in the GSA Year 2000 Warranty clauses, http://www.itpolicy.gsa.gov/mks/yr2000/contlang.htm (Revised -- August 22, 1997), site visited on September 16, 1998.

B. Curtis

government contractors from the non-compliance of other IT, the unintended result is that the IT products may be deemed Year 2000 compliant when in fact they are unable to operate with other government-owned or procured Year 2000 compliant IT products. In effect, data exchanging difficulties among or between compliant systems may prove to be the exception that consumes the rule.

Although the government should not expect an IT contractor to vouch for the compliance of another vendor's product, the government likewise should not have to be content to have procured IT that will work properly *only* when operated by itself. GSA appears to have anticipated this problem, and recommends that agency specifications include sufficient information to avoid interoperability problems: "This may include specifying the actual date/time programming convention to follow in the development process."[339] The suggestion in FAR 39.106(b) that the procuring agency "describe existing information technology that will be used with the information technology to be acquired and identify whether the existing information technology is Year 2000 compliant" only partially addresses this problem. Identifying other IT as "Y2K compliant" for an IT contractor does not guarantee that it will successfully interface with acquired IT. The example above demonstrates that much. The key is for the government to identify the Y2K compliance and the technical solution employed to achieve that compliance so that the contractor can design his system to properly interface. Furthermore, agencies should go beyond the FAR's suggestion of describing *existing IT* to be interfaced with the acquired IT. Agencies should make sure they provide the IT contractor with the interoperability requirements of the government's existing IT items and every other IT item the government is acquiring or has plans to acquire if that IT is expected to exchange data with the contractor's IT. Only this level

---

[339] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.2, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

B. Curtis

of specification will give government agencies the assurance that the equipment they intend to use in combination will successfully interoperate.

3. *Risk Allocation*

Risk is a key issue with Y2K compliance. Prior to the FAR compliance requirements, IT contractors were almost uniformly unwilling to make assertions regarding their products' Y2K compliance, and were uninterested in discussing their products' Y2K performance with potential customers.[340] Vendors would attempt to avoid any type of warranty of fitness for intended purpose by willfully remaining ignorant of the purposes for which government agencies desired to purchase their products. The FAR compliance requirement and the GSA Year 2000 Warranty forces manufacturers and vendors to address the compliance status of their products.

The GSA has proclaimed the new FAR definition of "Year 2000 compliant" a success, stating that "[w]orking from the definition, both Government and industry understand what is required to be Year 2000 compliant."[341] This understanding is the fist step for minimizing risk overall and enables the parties to balance the risk fairly. Either the GSA Year 2000 Warranty clause or specifications can be used to mandate Y2K compliance; GSA provided specific cautions for those seeking to reach compliance through the use of specifications. "In drafting specifications that achieve a balance between requiring compliance to meet mission requirements and placing the appropriate degree of risk upon the contractor, agencies are strongly encouraged to solicit significant input and feedback from industry."[342] This is precisely the type of

---

[340] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998).

[341] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[342] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.2, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

situation which calls for discussions with industry as suggested in the recently revised FAR Part 15.

Agencies must draft specifications which accurately describe the products required to meet the agency's needs. This is particularly true when addressing the Year 2000 compliance requirement. It is not enough for the agency to cite the FAR's definition of "Year 2000 compliant" if a specific technical solution (programming convention) is required. Precision is also required in drafting specifications so as to avoid unnecessarily placing too great a risk on the contractor. If required to assume more risk than is reasonable, potential offerors may either build excessive costs into the contract price or refuse to compete on the contract altogether. Either way the government does not achieve maximum competition to get the best possible bargain in meeting its requirements.

4. *Time Element*

The interim and final versions of the FAR rule differed from the original version of the GSA warranty[343] in that they added the "time" element to "date/time data" in defining Year 2000 compliant.[344] Although none of those who submitted comments on the interim rule addressed this added element, ITAA submitted comments questioning the use of this term after the final rule was published.[345] ITAA asserted that FAR 39.002 was the first instance of the concept of time being interjected into the Y2K issue.[346] As explained to ITAA, some government agencies have data processing requirements that

---

[343] *GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests*, 38 Gov't Contractor (Fed. Pubs. Inc.) 3 (Sep 18, 1996) and the FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996 ("shall be able to accurately process date data).

[344] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, Jan 2, 1997.

[345] *See* ITAA FAR Comments, found at http://www.itaa.org/farcomments.htm, site visited on October 1, 1998. The comments were submitted September 22, 1997 and were subsequently amended, apparently after engaging in further discussions with government representatives regarding the purpose behind adding the time element to the compliance definition.

[346] ITAA FAR Comments, found at http://www.itaa.org/farcomments.htm, site visited on October 1, 1998. ITAA also pointed out that "the Institute of Electrical and Electronic Engineers (IEEE), an international standards body, is in the process of developing an industry-wide standard for Year 2000 terminology, to include the definition of Year 2000 compliant, which does not address the concept of time." *Id.*

B. Curtis

transcend time and that those requirements drove this portion of the compliance definition. ITAA proposed that these requirements be addressed "on an exception basis" rather than causing confusion for government and contractors alike by introducing the term "time" into Y2K compliance matters. Vendors have focused on Y2K as a date--not time--problem, and will probably be unwilling to reevaluate and retest the hundreds of thousands of "Y2K capable" products already on the market. The acquisition process may be impeded by introducing this new concept into IT contracting, at least until buyers and sellers understand how products need to meet Y2K "time" requirements. ITAA concluded that "time," apart from calendar dates, was not within the intent and scope of the rule and recommended the time element be removed.[347] The time element has been added to the GSA Year 2000 Warranty clauses and remains there and in the FAR definition.[348]

5. *Service Contracts*

Unlike the GSA Year 2000 Warranty clause which applies only to supply item acquisitions, the FAR Year 2000 compliance provisions also apply to IT service

---

[347] ITAA FAR Comments, found at http://www.itaa.org/farcomments.htm, site visited on October 1, 1998. In the alternative, ITAA suggested that GSA's Year 2000 Acquisition White Paper address the usage of the term. Neither the GSA White Paper (GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997), also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998) nor any other subsequent publication provides guidance on the usage to the term. Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 24, 1998). ITAA was aware of applications that "calculate 'date' by aggregating units of time with reference to a known time standard, but did not consider those applications "functionally different from the date calculations contemplated in the original Interim Rule approach." ITAA FAR Comments, found at http://www.itaa.org/farcomments.htm, site visited on October 1, 1998. Presumably ITAA meant the original GSA Year 2000 Warranty, rather than the interim FAR rule; the former did not include the time element while the latter did.

[348] The FAR Councils made several changes to the interim rule as suggested by ITAA, but has taken no action on this after the fact comment. ITAA typically speaks with force on various IT issues and the government is responsive because, according to ITAA's claims, "more than 90% of the [11,000] members we represent are currently engaged in some $10 billion in annual IT transactions with the Federal government; which amount may be significantly affected by the policies implemented by these rules." Comments from Marc A. Pearl, General Counsel & Vice President, Government Affairs, ITAA, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat).

B. Curtis

contracts.[349]   This is so because the compliance requirement applies "[w]hen acquiring *information technology*,"[350] and information technology is defined in FAR 2.101 as "includ[ing] computers, ancillary equipment, software, firmware and similar procedures, *services (including support services)*, and related resources."[351]   The DAR Council clearly understood the FAR Y2K compliance provisions to apply to IT service contracts: the Council concluded the compliance rules apply whether it is a contract to acquire "a new system or to *upgrade an older system*."[352]   In its comments on the interim rule, the Professional Services Council (PSC), which represents professional and technical service firms who perform IT services, made the connection between FAR 39.106, which facially appears to apply only to products,[353] and the definition of information technology in FAR 2.101, which obviously includes contracts for services.   PSC characterized the FAR 39.002 Year 2000 performance requirement as a warranty provision, stating that they "strongly believe that it is not appropriate to apply any warranty provisions to contracts let for the assessment or remediation of legacy systems and software to achieve Year 2000 compliance."[354]   The FAR's Y2K compliance requirements have been included in pure service contracts in addition to

---

[349] According to the principle architect of the FAR's Y2K provisions, FAR staff had discussed drafting a separate clause for IT services, but the focus of their charter was products and, most specifically, commercial off-the-shelf items. Although some language for an IT services clause was discussed, the plan was later discarded. Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998). With a definition of "information technology" that included services, agencies were able to use existing FAR provisions to contract for Y2K compliant IT services.

[350] FAR 39.106, *emphasis added*.

[351] FAR 2.101, *emphasis added*.

[352] DAR Council, "Explanation of FAR Language," *emphasis added*, posted at http://www.govexec.com/dailyfed/0298/020598bt.htm, site visited on September 25, 1998.

[353] FAR 39.106 does not include references to computers, equipment, hardware, software or firmware; yet, its stated application exclusively to "information technology that will be required to perform date/time processing involving dates subsequent to December 31, 1999" might lead one to believe that only equipment were at issue because only equipment (rather than services) could be information technology which performs date/time processing.

[354] Comments from Bert Concklin, President, Professional Services Council, March 3, 1997, in response to FAC 90-45 (March 3, 1997) (found in Case File 96-607 at the FAR Secretariat). "Given the uncertainty in both the condition of legacy software and the availability and accuracy of system, software and interface documentation, including source code," remediation service contracts should not contain a Y2K warranty, and the compliance definition presents liability risk akin to a warranty clause. *Id.*

product/service contracts and Y2K remediation contracts.[355] Industry providers might prefer to contract for "best effort" software remediation services, as PSC suggested,[356] but government agencies will understandably expect their remediation dollars to secure compliance rather than something possibly approaching compliance.

V. EMBEDDED TECHNOLOGY AND OTHER PROBLEMS

With all the good achieved by adding a definition of Year 2000 compliant and a compliance requirement to the FAR, these efforts leave several important areas of government procurement unaddressed or insufficiently addressed. The most serious problem is that the FAR's Y2K provisions do not apply to embedded technology, a coverage problem whose importance will become increasingly obvious as the full extent of embedded processing becomes more well known. Also, the interoperability exception to the FAR's Y2K performance requirement may be interpreted broadly, so broadly in fact that no meaningful performance standard remains. Lastly, because Y2K compliance is required only in government acquisitions of IT if that IT will be used to process millennial date data, the government may be acquiring IT which will fail in 2000 or later due to an embedded--but not used--date function.

A. SCOPE OF EMBEDDED TECHNOLOGY ISSUE

When the FAR Information Technology Committee was drafting the Year 2000 compliance definition and requirement provisions, the Committee recognized "the Year 2000 problem" is "[n]ot restricted to just mainframe, personal (PC), or notebook computers," but actually "has a broader impact. Many activities are really the result of

---

[355] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998).
[356] In fact, the commenter suggested "contractual ('best effort') coverage as a preferable option to warranty provisions. Comments from Bert Concklin, President, Professional Services Council, March 3, 1997. The comments on remediation services were somewhat unclear given that the interim rule neither required Year 2000 compliance in information technology remediation contracts nor did it include warranty provisions for any contracts.

B. Curtis

computerized applications."[357] The computers controlling those "many activities" are most often embedded processors. Embedded chips are found in electronic financial transaction systems, telecommunication systems, air traffic control systems, weapon systems, automated systems, industrial process controllers, medical devices, household appliances, automobiles, traffic signaling devices, video equipment, and a wide array of commercial products and components. Each item that uses embedded IT is potentially as susceptible to Y2K problems as non-embedded systems. GSA's application and implementation guide also recognized that the Year 2000 problem encompassed more than just computer software: "in addition to traditional computers and software programs, the scope of the Year 2000 problem is very broad and may impact any device with a microchip."[358] GSA noted that because microchips are present in so many types of equipment, "fixing the Year 2000 problem can be exceedingly complex to correct in some circumstances."[359] Even those attempting to maintain a guardedly-optimistic view regarding what the new millennium will bring have special concerns about the risks posed by embedded processors.[360]

President Clinton has made it clear that the Year 2000 problem involves microchips, on a large scale. While speaking at the National Academy of Science, the

---

[357] FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[358] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998.

[359] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 3, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. In addition to the typical legacy computer system, "[l]ocal area network and interface devices, telecommunications systems, traffic lights, automobiles, aircraft, elevators, ATM machines, biomedical devices, household appliances[,] etc., are also susceptible and unless fixed in a timely manner may also fail to properly operate when faced with dates after December 31, 1999." Id. Each of these examples serves to highlight how extensively microchips have permeated our society and the extent to which we would have to go to address every microprocessor that might potentially be affected by the Year 2000 problem.

[360] Steve Hewitt (steve@ccmag.com), Year 2000 Bug Part 1, The Challenge Ahead! CHRISTIAN COMPUTING MAGAZINE, Volume 10 , Issue 9, Sep 1998, found at http://www.gospelcom.net/ccmag/articles/tele0998.shtml, site visited on October 23, 1998. "Even if we solve all of the software problems, what will chips with clocks embedded in them do when the year 2000 rolls around?"

president said that "Because the [Y2K Problem] is as far flung as the billions of microchips that run everything from farm equipment to VCRs, this is not a challenge that is susceptible to a single government program or an easy fix."[361] He noted that the conversion process is not limited to computer networks, but extends to the billions of microchips embedded into so many products we use on a daily basis. The growth of computing power also contributes to the present situation, the president pointed out, so that the "typical family home today has more computer power in it than the entire MIT campus had 20 years ago." The same is true in industry, where the president pointed out that as many as 10,000 individual microprocessors may be included in a single oil drilling rig. Months later, as he was signing the Year 2000 Information and Readiness Disclosure Act into law, the president commented that the Year 2000 Problem "may cause computers and embedded systems that run America's critical infra-structure to malfunction or even shut down."[362] Embedded processors are like the 90 percent of the iceberg that remains largely invisible below the surface of the water; the embedded processors around us are not often visible, so that we may remain unaware of their presence and critical functionality right up until they fail.

Embedded technology refers to embedded microprocessors or microchips ("chips") that have been integrated into some larger product or piece of equipment. That larger item may itself be information technology or it may be totally unrelated to computers, but for the embedded processor it contains. "There are literally billions of embedded microchips, most of which cannot be reprogrammed. Embedded chips often control processes within plants, refineries, manufacturing facilities, and run

---

[361] Remarks by the President concerning the Year 2000 conversion, delivered to the National Academy of Sciences (July 14, 1998), and found at http://www.y2k.gov/new/presy2k.html, site visited on October 3, 1998.
[362] Statement by President William Jefferson Clinton upon signing S.2392, the "Year 2000 Information and Readiness Disclosure Act," October 19, 1998, found at http://y2ktimebomb.com/WI/JW/wi9842.htm, site visited on October 21, 1998.

B. Curtis

sophisticated equipment."[363]   The Gartner Group, most frequently quoted for its estimates of Y2K remediation cost, "estimates that somewhere between 20 million and 250 million embedded systems failures could occur due to Y2K problems."[364]   The United Kingdom's Institution of Electrical Engineers has been trying to make people more aware of the importance of embedded technology through articles posted on the Internet:

> Any article on the Year 2000 problem in computers which appears in the general press should mention embedded systems, because there are very many more of them than there are computers, and because many companies (particularly smaller manufacturers) are much more liable to have a failure which seriously affects their business in an embedded system than in a computer.[365]

The power utility industry provides a stunning example of the role embedded technology plays in our national economy.   In a June 12, 1998 press release, the Senate Special Committee on the Year 2000 announced the results of a survey taken to measure the Y2K preparedness of ten of the nation's largest utility companies.[366] All ten of the surveyed companies had formal Y2K project plans, but eight of the utilities had not yet completed the initial assessments of their automated systems. This was especially true regarding embedded systems where four of the companies did not even have a tally of the number of embedded systems they were currently operating. The larger power utilities have automated their production and generation facilities and, in fact, their entire operations, using computers to control the automated systems. The surveyed companies were no exception to this practice, each reporting that they

[363] Linda A. Monica, *Year 2000 the Gathering Storm of Litigation of the "Millennium Bug,"* 13 ME. B.J. 184 (1998).

[364] Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998), found at http://www.cfcministry.org/library/Y2K/CFCposition/cfcY2Kposition.htm, site visited on October 23, 1998, *citing reference in* Bruce Webster and Paula D. Gordon, *A Call to Action: The National and Global Implications of the Year 2000 Embedded Systems Crisis*, Year 2000 Information Center, June 1998, found at http://www.year2000.com/archive/action.html.

[365] *Year 2000 and Embedded Systems*, found at http://www.iee.org.uk/2000risk/w-15.htm, site visited on October 27, 1998.

[366] *See* Y2K Committee Announces Survey Results Measuring Y2K Preparedness of Nation's Largest Utilities, found at http://www.senate.gov/~bennett/pr0612c98.html, site visited on October 21, 1998. The survey included gas, oil, and electric producers.

B. Curtis

employed automated systems in substantial numbers, and one of whom operates over 300,000. Embedded systems are an integral part of most automated systems, providing sensing, monitoring, measuring, management, switching and controlling functions throughout the typical power complex. The companies reported that mission critical systems represented somewhere between one-third and one-half of the overall systems. There was a great disparity between the number of embedded systems reported by the six utilities who have finished identifying them. Assessments of the embedded systems have lagged behind those of the other systems, largely "because *the problem in embedded systems was not apparent until recently.*"[367]

If 80% of the ten largest utility companies in the United States had not even completed their initial assessment of their computer-controlled automated systems by mid-1998, what is the likelihood that these companies will be prepared to provide uninterrupted power services at the turn of the century? In view of the time remaining before January 1, 2000, many companies should be heavily engaged in contingency planning. The surveyed utilities have not made sufficient progress in contingency planning either; none has a finished plan.[368] The good news, if there is any, is that the utilities already have plans for emergency response and disaster recovery, developed apart from the Y2K issue due to the criticality of the services they provide. The bad news is that these standing plans may not provide any relief if a Y2K problem is at the root of the failure.

An expert on microprocessor use in power facilities described the situation as follows:

> Within a typical electric utility, embedded logic control is prevalent in every facet of operation; from load dispatch and remote switchyard breaker control to nuclear power plant safety systems and fossil plant boiler control systems.

---

[367] Y2K Committee Announces Survey Results Measuring Y2K Preparedness of Nation's Largest Utilities, found at http://www.senate.gov/~bennett/pr0612c98.html, site visited on October 21, 1998, *emphasis added.*
[368] *Year 2000 and Embedded Systems*, found at http://www.iee.org.uk/2000risk/w-15.htm, site visited on October 27, 1998.

B. Curtis

Whole generating units (generally, gas turbines) are controlled from miles away by personnel adjusting system loads in response to peak demands. Embedded logic control is the dirty little Y2K secret of all production facilities (manufacturing and utilities) that has the most significant potential to bring whole companies to their knees.[369]

The utilities' experience is truly representative of the Y2K mindset that has predominated remediation efforts to this point: embedded systems have been overlooked and are only now being seen as a vastly important part of any effort to achieve an effective Y2K posture.

B. EMBEDDED TECHNOLOGY CARVED OUT

Embedded technology is clearly part of the Y2K problem and has been repeatedly acknowledged as an important segment of that issue; however, agencies, committees and reports have failed to address embedded IT when planning for the Year 2000. The FAR IT Committee reported that date-sensitive computers are used in many important computer systems throughout our culture, but did not specifically discuss embedded IT.[370] When GSA published its guidance on the newly finalized FAR provisions on Year 2000 compliance, it recognized that Y2K reaches far beyond the software programs operated on mainframe and personal computers and affects microprocessors in a myriad of applications.[371] Yet, GSA did not specifically discuss embedded information technology or how the new FAR provisions dealt with embedded IT. Considering that the "information technology" definition was not finalized in the FAR until December 9, 1997, it is possible that the GSA staff had no reason to know that

---

[369] Rick Cowles, *Electric Utilities and Year 2000, Embedded Logic and Controls,* found at http://www.euy2k.com/embedded.htm, site visited on October 20, 1998. Cowles' biography includes testifying at congressional Y2K hearings and appearing on nationally syndicated media programs, working in various capacities in the power generation industry, and specialization in the Y2K Problem as it relates to microprocessor technology in control systems. His complete biography is available at http://www.euy2k.com/contact.htm, site visited on October 20, 1998.

[370] *See* FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996.

[371] *See* GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 1.1, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. "The problem is not limited to software programs. Some hardware, firmware, and microchips may not be able to process dates after December 31 1999."

B. Curtis

embedded technology would be treated any differently than other IT. When GSA's FAR guidance was published in August of 1997, the interim FAR definition of information technology could be (and had been) interpreted to include items with embedded technology.[372] Therefore, GSA staff may have thought that embedded technology would be subject to the FAR Y2K compliance requirements. It is more likely, however, that the drafters simply failed to consider how embedded technology would be treated under the new Y2K rules, and with good reason. The instructions from the Chief Information Officer (CIO) Council's Subcommittee on the Year 2000 were to address the Y2K compliance of IT.[373] Historically, the term "information technology" had not been used to denote embedded IT, so the staff members drafted compliance provisions that had meaning only in reference to IT, but did nothing to define that term differently from the FAR 2.101 definition.

1. *"Information Technology" Defined*

Prior to August 8, 1996, the FAR did not contain a definition for "information technology."[374] A definition was added as a means of implementing a portion of the

---

[372] *See* Comments from Gary Krump, Department of Veterans Affairs, Deputy Assistant Secretary for Acquisition and Materiel Management, in response to FAC 90-41 (October 7, 1996) (found in Case File 96-319 at the FAR Secretariat). "The definition for information technology can be interpreted to include medical equipment such as Computerized Tomography (CT) scanners and Magnetic Resonance Imaging (MRI), which rely on integral computers." *Id.*

[373] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998).

[374] In 1995, the FAR did not contain a definition for the term "information technology," although the term occurred thirty-three times within the Code of Federal Regulations, one of which was in the DFARS. Most of the occurrences were merely portions of an address, or identified a government entity, or referred to the Information Technology Fund. Several directed federal agencies to create, maintain, and update five-year plans regarding the acquisition of "information technology" or "federal information processing" resources and replacement of outdated resources. However, in the DFARS reference "information technology" was included as part of the definition of "automated information system." 48 C.F.R. 239.7501-1, 1995. Embedded technology was not discussed in this definition, but the definition for "major automated information system" excluded "automated information systems which are an integral part of a weapon or weapon system, test support for a weapon or weapon system, or information technology basic research and development." *Id.* This exclusion for weapon systems is historically typical and is discussed further below.

B. Curtis

Information Technology Management Reform Act (ITMRA).[375] One of the most important features of ITMRA was that it repealed the Brooks Act, which had made GSA the exclusive procurement authority for most computer acquisitions, and returned authority to each executive agency to make its own IT acquisitions.[376] ITMRA was part of a congressional effort to improve the way the government acquired and managed IT, attempting to streamline and simplify the acquisition procedures.[377] One provision of ITMRA established the following definition:

> (3) Information technology
>
> (A) The term "information technology", with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
>
> (B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
>
> (C) Notwithstanding subparagraphs (A) and (B), the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.[378]

This definition was rather encompassing and was certainly broad enough to include embedded processors. Whether considered hardware, as physical devices, or software, due to the instruction logic contained therein, embedded processors fit the

---

[375] Information Technology Management Reform Act, 1996, Pub. L. No. 104-106, §5001, 110 Stat. 186, 679 (1996). ITMRA was passed into law on February 10, 1996 as part of the Information Technology Act which was, itself, part of the National Defense Authorization Act for Fiscal Year 1996. The Act has since been amended and is now referred to as the Clinger-Cohen Act of 1996.

[376] Information Technology Management Reform Act, 1996, Pub. L. No. 104-106, §5001, 5105, 110 Stat. 186, 679 (1996). Section 5105 repeals section 111 of the Federal Property and Administrative Services Act of 1949, as amended (the Brooks Act) (40 U.S.C. 759).

[377] See FAC 90-41; FAR Case 96-319; Item I; 61 FR 41467, Aug 8, 1996.

[378] 40 USC § 1401, 110 Stat. 679, Public Law 104-106, Division E, § 5002 (February 10, 1996).

"any equipment or interconnected system or subsystem of equipment" portion of the definition. Furthermore, embedded processors are used in a wide range of applications which include most--if not all--of those included in the definition. Considering how embedded processors are frequently used in control and processing equipment where they function automatically, rather than at the direction of a user, it could be argued that embedded technology fits the definition of information technology better than some non-embedded computer equipment. Microprocessors are computers, contain software, and are sometimes considered "firmware"[379] because they function like hardware, but in some cases have the ability to be reprogrammed like software. No imagination is required to see that embedded technology meets ITMRA's definition of "information technology."

To implement ITMRA, the FAR Councils agreed to amend the FAR by, among other things, adding a definition of "information technology" to FAR 2.101.[380] The FAC was published on August 8, 1996, nearly six months after the passage of ITMRA on the precise date when the Act became effective. The preambulary language in the circular stated that the purpose for this implementation was to "provide a simplified, clear, and understandable process for acquiring information technology (IT) that addresses the management of risk."[381] As was the case with the publication of the FAR Year 2000 compliance rules, the interim rule adding the definition of "information technology" to the FAR was promulgated before allowing the statutorily required period for public comment. The preamble to the circular justifies this unusual action, stating the "compelling reason" that "the ITMRA, passed February 10, 1996, should be effective by

---

[379] As noted above, firmware is "[s]oftware on a chip; programs stored on ROM [(read only memory)] chips, as distinguished from software programs stored on tapes or diskettes." JAMES V. VERGARI AND VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER--HIGH TECHNOLOGY LAW (American Law Institute - American Bar Association Committee on Continuing Professional Education 1991) at 608.
[380]FAC 90-41; FAR Case 96-319; Item I; 61 FR 41467, Aug 8, 1996.
[381] FAC 90-41; FAR Case 96-319; Item I; 61 FR 41467, Aug 8, 1996.

B. Curtis

August 8, 1996. Regulations should be in effect by that date."[382] As required by law, there was a period for public comment after the interim rule went into effect but before the rule was published in final form.

The interim rule added the following definition to FAR 2.101:

> Information technology means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
> (a) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency which--
> (1) Requires the use of such equipment; or
> (2) Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
> (b) The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
> (c) The term information technology does not include any equipment that is acquired by a contractor incidental to a contract.

The FAR definition made very few changes to the language taken from ITMRA, none of which affect the meaning of the definition relative to embedded technology. Much like ITMRA, the interim FAR definition of "information technology" is silent regarding embedded IT.[383] For all of the reasons mentioned above, embedded processors would qualify under the interim FAR definition.

The final rule for the FAR definition was published over 16 months later on December 9, 1997. In the meantime, both the interim and final rules for the Year 2000

---

[382] FAC 90-41; FAR Case 96-319; Item I; 61 FR 41467, Aug 8, 1996. The preamble does not, however, indicate why no interim rule was proposed for public comment during the intervening period between when the ITMRA was enacted, February 10, 1996, and the effective date, August 8, 1996. The most likely reason was the additional administrative process involved in coordinating with and between the FIRMR Transition Committee in addition to the CAA Council and the DAR Council. Also, the entire regulatory framework of the FIRMR was being replaced by what the FAR Councils were adding to the FAR.

[383] It may seem contradictory (at worst) or violative of the rule against using a term to define itself (at best) to describe embedded processors as "embedded information technology" when discussing whether or not such processors are included in or excluded from a definition of "information technology." However, embedded processors are labeled as "embedded information technology" or "embedded IT," even when being excluded from the definition of IT, probably because that term nonetheless communicates the processor's nature as a computing device. See 48 C.F.R. 2.101 ("The term information technology does not include-- . . . [a]ny equipment that contains [e]mbedded information technology").

compliance provisions had been added to the FAR. The preamble to the final rule declared that in addition to streamlining and simplifying the IT acquisition process, the rule "minimizes the economic burden of such acquisitions, while expanding opportunities for small entities to participate in Federal information technology contracts."[384] The final rule made the following changes to the interim rule:

> Section 2.101 is amended in the definition of "Information technology" by revising paragraph (c) to read as follows:
>
> 2.101 Definitions.
>
> Information technology
> (c) The term information technology does not include--
> (1) Any equipment that is acquired by a contractor incidental to a contract; or
> (2) Any equipment that contains imbedded [sic] information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

The background section of the circular explained that the FAR Councils considered all twelve comments received from the four respondents during the public comment period and that the definition of information technology "has been clarified" in response to those comments.[385] The only comment received that dealt with the definition of information technology came from the Department of Veterans Affairs (VA) who opposed the interim definition because it "can be interpreted to include medical equipment such as Computerized Tomography (CT) scanners and Magnetic Resonance Imaging (MRI), which rely on integral computers."[386] The VA suggested that the IT definition be modified to explicitly exclude medical equipment and offered a

---

[384] FAC 97-03, FAR Case 96-319; Item II, 62 FR 64914, Dec 9, 1997.
[385] FAC 97-03, FAR Case 96-319; Item II, 62 FR 64914, Dec 9, 1997.
[386] Comments from Gary Krump, Department of Veterans Affairs, Deputy Assistant Secretary for Acquisition and Materiel Management, in response to FAC 90-41 (October 7, 1996) (found in Case File 96-319 at the FAR Secretariat).

B. Curtis

definition of medical equipment that could be added to the FAR.[387] In responding to the VA's concerns, the FAR IT Committee stated that "[t]he definition of IT was not intended to include medical equipment such as CT scanners."[388] Rather than exclude medical equipment specifically, the Committee decided to "add clarifying language to the FAR which would note the exclusion of certain types of equipment which contain imbedded [sic] computers but, whose main function is not to process data."[389]

The "clarifying language" goes far beyond what the VA requested and carves out all embedded technology, unless that embedded IT happens to be integrated into an item that independently qualifies as IT. The definition properly identifies embedded microprocessors as IT, but the exception distinguishes embedded IT based upon the function of the equipment into which it is integrated. If the "principal function" of the equipment is something other than handling data or information in one of the enumerated ways, the equipment does not qualify as IT. For illustrative purposes, the rule gives several examples: thermostats or temperature control devices (whose principal function is regulating the temperature) and medical equipment (whose principal function is diagnosing, monitoring, or treating people) do not qualify as IT, regardless of the amount or complexity of the IT that has been integrated into those items.

---

[387] Comments from Gary Krump, Department of Veterans Affairs, Deputy Assistant Secretary for Acquisition and Materiel Management, in response to FAC 90-41 (October 7, 1996) (found in Case File 96-319 at the FAR Secretariat). The VA proposed that medical equipment be defined as "[d]edicated equipment or equipment systems which are intended for and designed to directly or indirectly provide for the monitoring, diagnosis or therapy of patients in the health care setting, and/or dedicated equipment or equipment systems which require Food and Drug Administration (FDA) approval as a medical device before it can be commercially marketed to health care providers." *Id.*

[388] Memorandum from Lawrence Wolfe, Chairman, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (February 4, 1997), containing the FAR IT Committee Report on FAR Case 96-319 (found in Case File 96-319 at the FAR Secretariat).

[389] Memorandum from Lawrence Wolfe, Chairman, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (February 4, 1997), containing the FAR IT Committee Report on FAR Case 96-319 (found in Case File 96-319 at the FAR Secretariat).

B. Curtis

It is possible to quibble with the "principal function" method of distinguishing embedded IT given the novel, if not ingenious, ways in which computers are employed today. Industrial applications sometimes use PCs as part of an automated manufacturing system to control machinery or robotics, for example, in some part of the process.[390] The PC may be integrated into the system much as a microprocessor is integrated into a temperature control device. The PC **acquires** information about where the next part is on the conveyor system, and **stores** that information for comparison (**manipulation**) to a desired operating range. As the part reaches the proper area, the PC **switches** on robotics equipment and **controls** it through a sequence of actions while sending system status information to a **display** panel. Before completing the operation, the PC **transfers** the data is has been **managing** to the next set of equipment down the line, **transmitting** and **receiving** data and serving as a **data interchange** between system components. The PC is integrated into a system whose "principle function" is to produce automobile parts, yet the PC is performing not just some, but perhaps all of the functions typically ascribed to "information technology." Would the PC be considered IT? Yes, but probably because it is a PC, rather than because of how it is being used.

Likewise, a temperature control device may have processors integrated into it to provide significant functionality. The device **acquires** information from sensors, determining the temperature in the surrounding environment and **displaying** that temperature. The temperature information is compared (**manipulated**) to the desired temperature value **stored** in the system. If the temperature is too low, a signal is sent to **switch** the furnace burners on, and that data is **managed** so that once the temperature in the furnace reaches a predetermined limit, the blower motor is engaged. The device **controls** the blower, turning it on and off depending upon the temperature

---

[390] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

B. Curtis

in the heat exchanger and the temperature in the environment being heated. Throughout the process, temperature and control signal data is **transmitted** and **received** in a rather dynamic data **interchange**. Without too much imagination, it is demonstrated that a temperature control device exhibits all of the characteristics of "information technology." Should it not be considered IT simply because its "principal function" is regulating temperature?

What these examples demonstrate is that a line between what will and will not be considered IT is arbitrary if it is based upon the "principal function" of the equipment. More importantly, whether or not the principal function of the item is an "information technology" function, nobody wants the equipment to stop working properly when the date rolls over to 2000.

2. *Omission by Design or Oversight?*

The hindsight available a year after the "information technology" definition was finalized in its revised form allows one to pose the question whether the embedded IT was omitted by design or oversight. The carve-out appears more purposeful when one considers that the embedded technology exception was the only revision in the final rule. Still, the question remains whether those who drafted the revision considered the ramifications of that choice as related to the Year 2000 Problem. One early comment on the rule change thought the answer was still uncertain: "It is not clear whether the drafters of the amended 'information technology' definition were aware of the effect it would have on the scope of the FAR Year 2000 rule."[391]

ITMRA's definition of "information technology" does not exclude embedded processors; therefore, it was not necessary for the FAR Councils to have excepted embedded technology from the IT definition. However, the distinction drawn between computing devices that are embedded and those that are not is a historical one,

---

[391] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) at 9.

B. Curtis

following along the rules that the government developed as it defined how agencies would acquire and manage computing equipment.[392]   The Federal Information Resources Management Regulation (FIRMR) was the regulatory scheme for acquiring and managing IT as authorized under the Brooks Act.[393]   The FIRMR had carved out embedded IT through a slightly different means, exempting it from FIRMR coverage rather than excluding it from the definition of IT.[394]   If the embedded IT could be used apart from its host equipment only after substantial modifications, or the value of the embedded IT was either under $500,000 or less than 20 percent of its hosts total value, the FIRMR did not govern its acquisition, management or use of the item.

The current chair of the FAR IT Committee recounted that as the FIRMR was being developed, the DoD did not want its operational, security, and cryptologic systems governed by those regulations.[395]   In his view, the DoD position was based partly on the Department's desire for independence, but more so on the distinction between the types of systems it operated.   He explained that many DoD IT systems, embedded or otherwise, were "real-time" systems, characterized as "hard science"

---

[392] Telephonic interviews with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 24, 1998), and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

[393] The FIRMR was found at 41 C.F.R. 201, but has since been revoked, pursuant to ITMRA.

[394] The FIRMR used the term "federal information processing equipment," or FIP, rather than "information technology." *See* 41 C.F.R. 201-1.002-2, 59 FR 66203, Dec. 23, 1994. The pertinent portion of the exception section read as follows:

(f) The FIRMR does not apply to the acquisition, management, and use of products containing embedded FIP equipment when: (1) the embedded FIP equipment would need to be substantially modified to be used other than as an integral part of the product, or (2) the dollar value of the embedded FIP equipment is less than $500,000 or less than 20 percent of the value of the product, whichever amount is lower. Embedded FIP equipment is FIP equipment that is an integral part of the product, where the principal function of the product is not the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. In an acquisition where multiple products are acquired, the exception applies to each discrete product.

(g) The FIRMR does not apply to the acquisition, management, and use of FIP resources that will be used in or as embedded FIP resources (equipment, software or supplies) in products excepted from FIRMR coverage under s 201- 1.002-2(f). This exception includes replacement or upgrades of the embedded FIP resources, regardless of the cost.
41 C.F.R. 201-1.002-2 (f)-(g), 59 FR 66203, Dec. 23, 1994.

[395] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998). The majority of this paragraph results from the discussion that occurred during this interview.

technology, but that data-processing and data-base applications are characterized as "soft science" technology. The latter type of technology is more reasonably regulated as IT because there is more standardization in equipment requirements and projected applications, whereas the "hard science" technology needs are more diverse and require a great deal more flexibility in the procurement process. This historical picture serves as a backdrop to those who were crafting the FAR's IT definition.

As a result of ITMRA's repeal of the Brooks Act, the FIRMR was also repealed.[396] With the repeal of the FIRMR, any provisions from that regulatory scheme deemed still necessary were to be added to the FAR. The FIRMR Transition Committee worked with the FAR Councils to ensure the effective transition. The "principal function" language used in the FAR's embedded technology exception are taken straight from the FIRMR exception. Although there was no requirement for the FAR to exclude embedded technology, the historical setting and effort to transfer portions of the FIRMR to the FAR, along with the public comment from the VA, helps to explain how embedded technology was carved out of the FAR's IT definition.[397]

An examination of the timeline for the pertinent additions and revisions to the FAR may be helpful in understanding how the interaction of the rules may have been overlooked:

August 8, 1996, FAC 90-41[398] published the interim rule adding a definition of "information technology" to the FAR.[399] The definition was worded broadly enough to include embedded technology.

---

[396] 61 FR 39359, July 29, 1996, removed 41 C.F.R. Chapter 201, Federal Information Resources Management Regulation, effective August 8, 1996.

[397] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998). In fact, the FIRMR does not apply to radar, sonar, radio or television procurements; the CIA's IT procurements; and DoD IT acquisitions for intelligence and national security (crpytologic) activities, command and control functions, and components to be integrated into weapon systems. See 41 C.F.R. § 201-1.002-2(a)-(b).

[398] FAC 90-41; FAR Case 96-319; Item I; 61 FR 41467, Aug 8, 1996.

[399] 48 C.F.R. 2.101, Aug 8, 1996.

130   B. Curtis

January 2, 1997, FAC 90-45[400] published the interim rule adding a definition of "Year 2000 complaint"[401] to the FAR and the requirement to acquire only compliant IT.[402]

August 22, 1997, FAC 97-01[403] published the final rule, revising the definition of "Year 2000 compliant" and retaining the compliance requirement. Both sections of FAR Part 39 reference "information technology."

December 9, 1997, FAC 97-03[404] published the final rule, revising the definition of "information technology" to exclude embedded IT.

When the interim IT definition was published, there were no FAR provisions on Y2K compliance to consider. When the Y2K compliance provisions were added to the FAR, citing their applicability to "information technology," that term had been defined broadly enough to encompass embedded technology. By the time the final rule was published, amending the IT definition, the FAR Y2K compliance provisions had been in place for about three and a half months. Since it was the same CAA Council and DAR Council approving these rules, one might expect that they considered the effect of the definition change on the Y2K rules they had so recently finalized. The FAR IT Committee's report, recommending the embedded technology exclusion, was sent to the FAR Councils on February 4, 1997. This significance of this date can be viewed from two perspectives: 1) The decision to exclude embedded IT was made ten months before the final rule was published, so that all of the intervening actions with respect to Y2K compliance were not reconsidered before the revision was published. 2) The decision to exclude embedded IT was made only one month after the Y2K compliance provisions had been added by interim rule, so that the revision certainly considered the potential impact upon Y2K compliance requirements.

---

[400] FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, Jan 2, 1997.
[401] 48 C.F.R. 39.002, Jan 2, 1997.
[402] 48 C.F.R. 39.106, Jan 2, 1997.
[403] FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44830, Aug 22, 1997.
[404] FAC 97-03, FAR Case 96-319; Item II, 62 FR 64914, Dec 9, 1997.

B. Curtis

Shifting the focus to the Y2K compliance rules, the drafters could have ensured the government made the same compliance demands on vendors with IT embedded in their products that were made on IT contractors. In fact, the Y2K compliance provisions did not have to reference IT at all. Then, regardless of the type of computing device or the equipment in which it was integrated, that computing device could not fail to function due to date-processing problems. Once again, the lead author of the Y2K clause that was provided to the FAR Councils stated that the drafters had been charged with creating a compliance clause that focused on commercial items contracts. He also pointed out that the vendors which deal with GSA's Public Buildings Service "would choke" if asked to certify compliance with the Y2K definition across the board for all the product lines they sold to the government.[405] Therefore, the more focused, practical approach was taken, dealing with IT, and then, only if that technology processed date data.[406]

The FAR staff who managed the administrative process of adding the Year 2000 compliance provisions to the FAR were surprised at how quickly they were able to get the interim and final rules through the CAAC and DARC and into the FAR.[407] The urgency of the situation was plain to Council members, and the rules received a great deal of priority and attention. Having been enacted quickly, so as to provide a standard designed to bring uniformity to federal IT purchases, it is not too remarkable that the FAR provisions did not anticipate every procurement situation.

In the final analysis, it appears that those who drafted both the IT definition and the Y2K compliance provisions, which necessarily refer to that definition, were

---

[405] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

[406] John Cornell reports that PBS was advised to ask vendors if their products track date data (not time-only systems) and, if so, GSA would instruct the vendor to insure the system was Y2K compliant. Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 24, 1998). Cornell suggests more information is available at http://www.gsa.gov/pbsintro.htm. *Id.*

[407] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998).

B. Curtis

operating under 1) the historical perspective: "we do not regulate embedded IT," 2) the predominant mindset of the day: "the Y2K implications of embedded technology are not very significant," and 3) a limited commission: "write rules for the acquisition of computers, focusing on commercial items. Omission by design or oversight, the effect is that embedded IT is not subject to the Year 2000 compliance requirements that apply to all other IT that will be used to process millennial dates.[408]

C. PROBLEM OF OMITTING EMBEDDED TECHNOLOGY

With the addition of a single subsection to the FAR's "information technology" definition, the FAR's mandate for government agencies to require Y2K compliance for thousands of items disappeared. The obvious ramification of removing (or failing to include) embedded IT in either the definition of IT or the Year 2000 compliance requirements is that government agencies may continue to procure items containing date-sensitive embedded IT that will not function correctly in the Year 2000. There may be other methods of protecting the government in such cases, but most of those methods existed prior to the FAR's Y2K provisions.

"Embedded systems are a potential Achilles heel, and widespread failure of these crucial systems threatens to cause severe financial harm . . . ."[409] The embedded IT issue is just as real and perhaps more serious than the portion of the Year 2000 Problem which relates strictly to software and larger scale computing systems. Those devices are easier to find. Remediation may involve millions of lines of code, but that code is generally easier to locate than the thousands of processors embedded in some facilities. Furthermore, each processor has its own software to check, and that software may have been made permanent (firmware) so that replacement, rather than software

---

[408] Richard Kellett's personal perspective is that there is no reason to have limited the Y2K compliance requirement to information technology. Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).
[409] David M. Nadler, *Embedded Systems--The Real Year 2000 Problem*, found at http://www.comlinks.com/legal/dnemb1.htm, site visited on December 10, 1998.

B. Curtis

conversion, is the only viable option. When compliance problems occur, they are easier to find and fix in large mainframe computing systems and even in personal computers. Where embedded processors are involved, part of the task is determining where the processors are and which one(s) caused the problem.

In 1998, the DoD Inspector General (IG) reviewed 16 DoD weapon system acquisition programs to determine whether the contracts and solicitations for contracts included Year 2000 compliance provisions as required by the FAR.[410] The Audit Report noted that Y2K compliance provisions were missing in 9 of the 16 weapon systems reviewed.[411] The DoD IG concluded that "the failure of the Program Management Offices to address the Y2K requirements in the contracts for weapon systems could result in greater costs to correct the problem in the future."[412] This is precisely the problem the FAR Year 2000 provisions were supposed to avoid: additional government cost to correct non-compliance problems.[413]

Today's weapon systems--including the armored vehicles, ships, aircraft, missile systems, and navigation and communication systems reviewed by the DoD IG--contain

---

[410] In an informal partnering arrangement with the DoD's Chief Information Officer, the DoD Inspector General has been monitoring the Department's progress as it addresses Y2K issues and has been publishing a series of reports on those efforts. More information about those reports is available at http://WWW.DODIG.OSD.MIL/audit/reports/index.html, site visited on December 1, 1998.

[411] OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, *Year 2000 Contract Language for Weapon Systems* (September 22, 1998), at 4. The Report notes that the audit preceded guidance from the Under Secretary of Defense for Acquisition and Technology on including Y2K compliance provisions in weapon systems. *Id.* However, the audit post-dated the DoD Year 2000 Management Plan which contained Assistant Secretary of Defense (C^3I) guidance on including Y2K provisions in contract provisions for national security system procurements. *See* DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998, found at http://www.dtic.mil/c3i/y2k/title.html, site visited on October 27, 1998. Following the DoD IG's Report, the Secretary of Defense issued a letter directing the Military Departments and DoD agencies to report on whether they have included Y2K compliance in the contracts and solicitations for their major system acquisitions. "The Secretary of Defense also directed that funds not be obligated for any contract that was for information technology or national security systems that process date-related information and that does not contain Y2K requirements specified in Section 39.106 of the [FAR]." OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, *Year 2000 Contract Language for Weapon Systems* (September 22, 1998), at 6.

[412] OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, *Year 2000 Contract Language for Weapon Systems* (September 22, 1998), at 6.

[413] *See* FAC 90-45; FAR Case 96-607; Item XIV; 62 FR 273, 274, Jan 2, 1997.

embedded technology in unprecedented numbers. Because the principal function of a weapon system--to kill people and break things--is not one of those listed in the "information technology" definition, the reviewed systems would not be considered IT as the FAR defines that term. The IG concluded that "[t]he development and acquisition of software, information technology systems, **and software embedded in weapon systems** that accommodate the century change is essential to future mission effectiveness."[414] If the Y2K status of our weapon systems is not timely addressed, whether due to lack of inspection and testing or because additional non-compliant weapon systems are acquired, the military systems we depend upon may not be able to accurately process date data after December 31, 1999. The result could be unpredictable system failures that cripple weapon systems stationed around the globe, impacting DoD missions and leaving the United States and those we defend vulnerable to attack.[415]

The potential for processor failure is neither hypothetical nor mere speculation. Such failures have already occurred. On December 30, 1996 at exactly midnight, all 660 process control computers at the New Zealand Aluminum Smelters plant shut down, bringing the production facility to a grinding halt without a moment of advance warning.[416] When the smoke cleared, literally speaking, the problem was traced to embedded processors that were not programmed to take into account that 1996 was a leap year. The computers did not recognize the additional, 366th, day and instead failed simultaneously at the end of the 365th day of the year. Less than 24 hours later, the problem had been fixed, but by that time over $1 million of damage had occurred. With process control computers off-line, the temperatures in the smelting equipment

---

[414] OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, *Year 2000 Contract Language for Weapon Systems* (September 22, 1998), at 2.
[415] *See* OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, *Year 2000 Contract Language for Weapon Systems* (September 22, 1998), at 2.
[416] EDWARD AND JENNIFER YOURDON, TIME BOMB 2000--WHAT THE YEAR 2000 COMPUTER CRISES MEANS TO YOU! (Prentice Hall PTR 1998), at 284.

B. Curtis

was left unregulated; some of the equipment was damaged beyond repair as a result of the overheating.[417]

The United Kingdom's Institution of Electrical Engineers warns that "[e]mbedded systems--and their failure--may affect not only business profitability but also the safety of employees, customers and the general public."[418] One report, commissioned by a United Kingdom executive agency, "predicts that there is a 10- 15% chance of the embedded chips in safety systems in engineering processes failing in year 2,000 unless action is taken to rectify the problem." This statistic becomes more frightening when one considers what this failure rate could mean world-wide for the 20 billion processors integrated into automated industrial equipment, transportation equipment and controllers, medical devices and systems, and consumer products used in the office and the home.[419]

Embedded processor failure also poses great risk for personal injury in the health care industry where a stunning array of equipment contains embedded IT. Microprocessors are commonly found in diagnostic, testing and monitoring equipment such as computer-aided tomography (CAT) scanners and magnetic resonance imaging (MRI) systems, laboratory equipment which measures the concentrations of numerous substances in blood and urine, and pulse-oxymeters which measure and monitor heart rate and the concentration of oxygen in the bloodstream.[420] Microprocessors are also used as process controllers in equipment which actually delivers medical care, such as defibrillators and pacemakers which regulate heart function, ventilators which assist in

---

[417] EDWARD AND JENNIFER YOURDON, TIME BOMB 2000--WHAT THE YEAR 2000 COMPUTER CRISES MEANS TO YOU! (Prentice Hall PTR 1998), at 284.

[418] *Year 2000 and Embedded Systems*, found at http://www.iee.org.uk/2000risk/w-15.htm, site visited on October 27, 1998.

[419] Robin Guenier, Task Force 2000 and former Government Millennium advisor, as quoted online at http://www.bbc.co.uk/education/disaster/bug.shtml, site visited on October 21, 1998. Commenting on the Health & Safety Executive's report, Guenier wrote that "Even the failure of a fraction of these could result in major accidents."

[420] These items are meant only as familiar illustrations of the myriad of medical equipment containing computer chips that provide vital functionality, rather than as an attempt to list all such equipment.

B. Curtis

breathing, infusers which deliver measured amounts of medication over programmed time periods, kidney dialysis machines which cleanse the blood, recirculation devices which oxygenate the blood and pump it through the patient while the heart is inoperative, closed-circuit television optic systems which allow for less-invasive surgery, and laser surgical instruments. As staggering as may be the total number of pieces of medical equipment at risk for Y2K failure, the enormity of the problem expands still farther when one considers the number of vendors that the typical medical facility may have to contact to determine the status of every piece of equipment. One particular medical facility reported having at least 2000 vendors for its over 15,000 medical devices in addition to the nearly 3000 vendors from whom the facility purchased supplies and services.[421] Apparently the medical supply industry is taking the Year 2000 Problem seriously, as evidenced by special Y2K remediation service companies directed particularly towards fixing medical technology devices.[422] Considering the high percentage of medical equipment which uses date-sensitive embedded technology, it becomes retrospectively ironic that it was the VA's request to exclude medical equipment from the definition of "information technology" that prompted the exclusion of embedded IT.

Those who drafted GSA's guidance for implementing the FAR compliance requirements perceived the need for medical devices to be Y2K compliant. In describing the particular need to address testing requirements in contractual Year 2000 specifications, the guide states the following:

> Based on the criticality of the system, an agency should specify in the solicitation the degree of testing necessary to ensure the product meets the requirement.

---

[421] EDWARD AND JENNIFER YOURDON, TIME BOMB 2000--WHAT THE YEAR 2000 COMPUTER CRISES MEANS TO YOU! (Prentice Hall PTR 1998), at 221.

[422] *See Millennia III Partners With Technology in Medicine, Inc. To Address Year 2000 Problems in Biomedical Devices* (June 17, 1998), found at http://www.year2000.com/releases/NFmilllII_6_17_1998.html, site visited on October 21, 1998. The press account announces the partnership between "Millennia III, Inc., a leading provider of comprehensive Year 2000 solutions, and Technology in Medicine, Inc., a leading provider of technology management and maintenance solutions of healthcare organizations." *Id.*

B. Curtis

For example, testing requirements for a medical system where failure to accurately process data could result in life threatening situations should be very rigorous.[423]

There may be a small ray of hope for some embedded systems. Part of the engineering process behind real-time systems development is contingency planning.[424] If designed correctly, a system will not fail in a catastrophic or harmful way even if the application or operating software performs improperly. One example of a contingency response would be having all burners in a steel refinery shut off automatically if process controllers stop sending signals to the system. Contingency analysis, including this sort of "fail safe" designing, is part of standard design planning, particularly where there is potential for loss of life, serious injury, or even excessive property damage. Some system developers, however, do not expend the time and resources to fully consider what could occur in the event of a technological failure. Furthermore, the success of a contingency plan rests in some degree on the ability of the designer to anticipate the failure which eventually occurs. We all hope the person who designed the elevator planned thoroughly and properly for how the elevator should react if the controller goes off-line. We also hope he considered how it should respond if the controller remains on-line, but provides the type of erroneous controls that could cause dangerous operation. Furthermore, some systems present dangers beyond the ability to provide effective fail safes, such as airplanes. If fuel stops flowing to the engines, some airplanes may be able to glide, possibly even to a safe though emergency landing. Other aircraft could anticipate only one thing in that same situation: the plane is going

_____

[423] GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000 FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997) at section 2.5.2, also found at http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998. This paragraph goes on to point out that a less critical application, such as an accounting system, would not need the same high level of compliance testing. The accounting system, however, would most likely be contained in a computer system which *would* fit the FAR definition of information technology; hence, the contract used to acquire the computer used for the accounting system would have included a Y2K compliance requirement, unlike the contract for life-saving medical equipment.
[424] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998). The majority of this paragraph comes either directly from the discussion that occurred during this interview or the thought processes that followed.

down--fast. Where "graceful degradation" is not possible, redundancy may be the only means of contingency planning: if one system fails, a "backup system" should take over. The Y2K Problem presents an unusual situation for contingencies where redundant "backup systems" are likely to suffer the same ills as primary systems.

Fortunately, the importance of embedded IT as a key aspect of the Year 2000 Problem is growing, signaled by the emergence of conferences and seminars strictly devoted to the problems posed by non-compliant embedded IT and the means for adequately addressing risks and remediation.[425]

D. NON-DATE-PROCESSING IT WITH DATE-SENSITIVE CHIPS

As has been discussed thus far, the FAR's Y2K compliance provisions do not apply to embedded technology, generally, whereas the GSA Y2K warranty does. Both the warranty and the FAR provisions are designed to ensure the government acquires computers and computer-related items that will function properly in the Year 2000. Both mechanisms require covered IT to perform accurate date processing at specified times under prescribed conditions.

Consider the following: what if a company which manufactures modems needs a microprocessor for its modem board to perform a specific application unrelated to date or time data.[426] The manufacturer selects a multi-purpose chip because it is far cheaper to use the required functionality available on a multi-purpose chip and disregard the unneeded capacity than it would be to commission a chip designer/manufacturer to produce a chip specifically tailored to the modem application. Suppose that one of the

---

[425] See, e.g. *Year 2000 and Embedded Systems*, October 15-16, 1998 conference sponsored by the Year 2000 Project; Texas Departments of Information Resources, Criminal Justice, Mental Health, Mental Retardation, Public Safety; Texas Youth Commission; the Federal Bureau of Investigation; the United States Department of Justice; and the Federal Bureau of Prisons, published at http://www.dir.state.tx.us/y2k/embedded/index.html, site visited on October 21, 1998.

[426] The scenario in this section was created based on more general information derived from telephonic interviews with Walter Benesch, Y2K Oversight Contingency Planning Office, Office of the Secretary of Defense, Command, Control, Communications and Intelligence (OSD/ C^{3}I), and Executive Secretary to the Defense Science Board Task Force on Year 2000 (October 19, 1998), and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).

B. Curtis

other functions available on that multi-purpose chip is a date/time function or counter. What will happen to the counter or clock or date function on that chip--although not being used by the modem board--after the stroke of midnight on December 31, 1999?

For those who conclude that all of these suppositions are a bit too hypothetical, the microprocessor market *does* include multi-purpose chips that provide a number of separate functions on the same chip, frequently including a date or counter function.[427] Such general purpose chips are selected for use on modem boards[428] and other applications, some of which use the date or counter function and some of which do not. What will occur when the clock on these chips reaches the Year 2000[429] is just as unknown as is the result awaiting any other non-compliant processor. What *is* different about these chips is that people will not be expecting any adverse results or processing failures from the systems in which these chips are integrated where the host equipment does not process date/time data.

In discussing embedded technology issues, the author was often asked how a product will be affected by Y2K if the product does not use date data. As an example, a programmable digital thermostat, used to adjust household temperature settings on various days of the week and times of the day, does not require the submission of a month, year or date in order to function properly. If no year has been input, how then will the thermostat be affected by the Year 2000 or any other external change.[430] The

---

[427] Telephonic interviews with Walter Benesch, Y2K Oversight Contingency Planning Office, Office of the Secretary of Defense, Command, Control, Communications and Intelligence (OSD/ C^3I), and Executive Secretary to the Defense Science Board Task Force on Year 2000 (October 19, 1998), and Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998); *see also* Mark A. Frautschi, (frautsch@tmn.com), *Embedded Systems and the Year 2000 Problem (The OTHER Year 2000 Problem)*, September 28, 1998 draft, found at http://www.tmn.com/~frautsch/y2k2.html, site visited on October 20, 1998. Frautschi deals with this embedded technology problem at great length and includes his a list of numerous Internet sites that he has found useful in researching this area of the Y2K Problem.
[428] Telephonic interview with Richard N. Kellett, Chair for the Joint FAR Information Technology Committee (October 27, 1998).
[429] The same type of problems could result when a counter reaches its boundary and "rolls over," as described in the section on data overflow.
[430] *See* Mark A. Frautschi, (frautsch@tmn.com), *Embedded Systems and the Year 2000 Problem (The OTHER Year 2000 Problem)*, September 28, 1998 draft, found at

response lies in the underlying microprocessor which is used to track time. Here again, due to the economies of using existing technology rather than commissioning the design of an application-specific processor, the thermostat probably uses a real time clock to track elapsed time. The controller needs to know how much time has elapsed since the last setting change to determine whether it is time to make the next setting change. The application only uses the time and day of the week function, but the clock in the processor most likely is providing full time and date counting. The month and year data is not used by the thermostat, yet the month and year portions of the count are advancing over time and will reach January 1, 00 (assuming a two-digit year field) at some point. The question with the thermostat is the same as with any other IT device: how will the software react to the "00" date?

To turn the focus of this scenario on the government's Y2K compliance provisions, we should consider what will occur when the government contracts to purchase some non-IT item that will not be required to process date/time data but,

---

http://www.tmn.com/~frautsch/y2k2.html, site visited on October 20, 1998. In e-mail correspondence Frautschi applied this explanation to an elevator scenario posed by the author. Elevators must be cycled through a bottom-to-top-to-bottom cycle periodically to reset the cables. The controller for this function can determine "have 12 hours elapsed?" by subtracting the start time from the current time and then compare the result (probably measured in seconds) to 12 hours. If the result is greater than 43200 seconds (12 hours), the controller initiates the reset process and begins counting time again, measuring for the next reset cycle. At initialization, the current time is written into a buffer called START. Current time is maintained in another buffer called NOW. The reset program will be set to perform the following computation periodically:

    IF (NOW - START > 43200) THEN
            (reset the elevator cables)
    ELSE
            (do nothing)
    END IF

With this formula, the START buffer would have to be reloaded to the current time at the end of each reset cycle. The problem will occur when time (NOW and START) use two digits to represent the year and the clock reaches January 1, 2000. The next time the controller checks to see if the cable reset routine should be performed, the buffers may span the century marker so that NOW = TIME/01/01/00 and START = TIME/12/31/99. When the processor runs through the computation routine, it will produce a negative result and the routine will never call for the cables to reset. One might respond that the problem could be solved by simply stripping the two-digit year portion off the clock data before loading it into the START and NOW buffers, but then the same "never reset" problem would occur at any year boundary. This same logic underlies numerous items that use clock or counter data for relative and actual time calculations.

B. Curtis

nonetheless, has one of these multi-purpose chips embedded inside that includes a date function. Under the GSA Year 2000 Warranty clause there is little doubt about whether or not an item has to function properly in the Year 2000: if the item is "listed," it will have to accurately process date/time data. Under this scenario, it is highly unlikely that the government would require a product to be "listed" when it is not looking for an item to process date/time data. In fact, unless the contract happened to include some IT item that would process date/time data, the contract would not even include the Year 2000 Warranty clause. If perchance, this multi-purpose chip were integrated into something that was itself considered computer equipment, such as a modem board, the warranty might be included and the item listed. Only in such a circumstance would the failure be covered by the contract's Y2K warranty provision.[431]

Under the FAR's Y2K provisions, the result is even worse. Because an item is judged by its principal function, rather than the technology it contains, an item which does not perform one of the enumerated IT functions as its principal function will not be considered information technology and, hence, the contract will not require Y2K compliance. The reason that the situation is worse under the FAR's Y2K provisions than the GSA warranty is because of how an IT item, such as the modem, will be treated. Although the modem would be considered IT under the FAR 2.101 definition, the contract still would not contain any Y2K compliance requirement. This is because FAR 39.106 only requires such a provision "[w]hen acquiring information technology that will be required to perform date/time processing." In our scenario, the modem board will not be required to perform date or time processing. So, where an agency is procuring what the government definition deems to be "information technology," that item may not be required to be Y2K compliant, even where a function operating on a microprocessor within that item may be date-sensitive.

---

[431] Obviously in any of these scenarios there might be other bases for contractual remedies. For the purposes of this section, the specific Y2K compliance provisions are being viewed in isolation to emphasize the lack of coverage that they provide to the government.

B. Curtis

These scenarios demonstrate the coverage problem with the GSA Year 2000 Warranty and the FAR Year 2000 Compliance provisions. Neither is effective against a real life Y2K problem. About the only situation where one of the government's Y2K solutions would be effective regarding one of these date-sensitive multi-purpose chips would be if it were integrated into some IT item which the government required to perform date/time processing. Then, and only then, would a Y2K compliance provision specifically be called for.

VI. LEGISLATIVE, EXECUTIVE AND AGENCY OPTIONS

The federal government, along with most private sector industries, has been slow in becoming aware of and responding to the Year 2000 situation and the problems that it poses. While recognizing IT as a cornerstone of modernization in education, commerce, science and industry, the executive branch was slow in sounding the alarm or proposing solutions to the Y2K problem. Members of Congress have called for the executive branch to take a greater leadership role to head off a computer crises on January 1, 2000,[432] but Congress itself made little progress towards providing statutory or regulatory solutions until the middle of 1996. To date, the executive branch has addressed the issue with several executive orders[433] and appointed a national Y2K Czar[434] to provide executive leadership. The Congress has passed several statutes

[432] Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998, at A4.

[432] Year 2000 Computer Software Conversion: Summary of Oversight Findings and Recommendatuons, H.R. Rep. No. 857, 104th Cong., 2d Sess. (1996), note 21.

[433] Executive Order 13011 of July 16, 1996, 61 FR 37657, Vol. 61, No. 140, July 19, 1996, was issued, in part, to implement the Information Technology Management Reform Act of 1996, including the establishment of the Chief Information Officers (CIO) Council to function "as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources." *Id.* It was the CIO Council that asked GSA to begin drafting Y2K warranty clauses and FAR provisions. FAR Information Technology Committee Report on FAR Case 96-607, October 28, 1996. Executive Order 13073 of February 4, 1998, 63 FR 6467, Vol. 63, No. 25, February 6, 1998, established the President's Council on the Year 2000 Conversion.

[434] In February of 1998, President Clinton appointed John Koskinen, formerly the deputy director for Management at the Office of Management and Budget, as the Chairman of the President's Council on the Year 2000 Conversion, which he had created via executive order.

B. Curtis

aimed at encouraging private industry to quicken its pace in addressing the issue and forcing government agencies to assess their status, create a remediation plan, and implement that plan in sufficient time to avoid disruption to mission-critical computing systems. As the critical date approaches, more legislation has been introduced to address various aspects of preparation for both government agencies and the private sector. It remains open to speculation what additional laws may be passed in the last few months preceding January 1, 2000, when the Year 2000 furor will have reached a fevered pitch.

A. "YEAR 2000 COMPLIANCE" REQUIREMENTS

This paper's focus is on the federal government's regulatory and legislative efforts to limit the Y2K Problem's impact as government agencies acquire commercial and non-commercial supply items. The majority of legislative, executive and regulatory actions regarding the Year 2000 Problem address funding,[435] remediation,[436] agency status and reporting,[437] information sharing,[438] and the formation of councils, committees and task forces to study or address a particular area of the Y2K Problem. Relatively few actions have been taken in the acquisition arena, and the more important of those have been discussed earlier in this paper. Several additional measures along with a brief explanation thereof are listed below.

1. *Fiscal Year 1997 National Defense Authorization Act*

During the same time period when the Interagency Committee on the Year 2000 was working with the IT industry to develop a reasonable, government-wide Year 2000 compliance standard, committees within the House of Representatives were holding

---

[435] *See, e.g.* Supplemental Appropriations and Rescissions Act, Pub. L. No. 105-174, 112 Stat. 58 (1998).
[436] *See, e.g.* Continuing Appropriations for Fiscal Year 1999, Pub. L. No. 105-240, 112 Stat. 1566 (1998); Higher Education Amendments of 1998, Pub. L. No. 105-244, 112 Stat. 1581 (1998).
[437] *See, e.g.* Higher Education Amendments of 1998, Pub. L. No. 105-244, 112 Stat. 1581 (1998).
[438] *See, e.g.* Year 2000 Information Readiness and Disclosure Act, 15 USC § 1 (Note), Pub. L. No. 105-271 (1998).

hearings on various aspects of the Y2K problem.[439] Following the hearings, which included testimony from both government and computer industry experts, Congress included provisions addressing the Year 2000 problem in the National Defense Authorization Act for Fiscal Year 1997.[440] Section 831 of the Act, titled "Year 2000 Software Conversion," Directed the Secretary of Defense to "ensure that, as soon as practicable, all information technology acquired by the Department of Defense . . . has the capabilities to process date and date-related data in 2000."[441] The House Conference Report stated that "[w]hile DOD contracting personnel are authorized to consider and accept offers for non-compliant products, this authority should be conditioned on the offerors providing and committing to a timetable whereby products

---

[439] The Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight convened on April 16, 1996 to address the question "Is January 1, 2000 the Date for a Potential Computer Disaster?" On September 10, 1996, House members conducted a joint hearing of the Subcommittee on Government Management, Information, and Technology of the Committee on Government Reform and Oversight and the Subcommittee on Technology of the Committee on Science to address the topic "Solving the Year 2000 Computer Problem." The House Committee on Government Reform and Oversight summarized these hearings in its sixteenth report to the 104th Congress, H.R. Rep. 104-857, September 24, 1996, H.R. Rep. No. 857, 104th Cong., 2nd Sess. 1996.

[440] Public Law 104-201 (HR 3230), 110 Stat. 2422 (1996). The text for the pertinent part of the Act is rather succinct:

SEC. 831. YEAR 2000 SOFTWARE CONVERSION.

(a) YEAR 2000 SOFTWARE CONVERSION.--The Secretary of Defense shall ensure that, as soon as practicable, all information technology acquired by the Department of Defense pursuant to contracts entered into after September 30, 1996, has the capabilities to process date and date-related data in 2000.
(b) ASSESSMENT.--The Secretary, acting through the chief information officers within the department (as designated pursuant to section 3506 of title 44, United States Code), shall assess all information technology within the Department of Defense to determine the extent to which such technology has the capabilities to operate effectively.
(c) PLAN.--Not later than January 1, 1997, the Secretary shall submit to Congress a detailed plan for eliminating any deficiencies identified pursuant to subsection (b). The plan shall include--
 (1) a list of affected major systems;
 (2) a description of how the deficiencies could affect the national security of the United States; and
 (3) an estimate and prioritization of the resources that are necessary to eliminate the deficiencies.

[441] Public Law 104-201, δ831(a) (HR 3230), 110 Stat. 2422 (1996).

B. Curtis

sold to the government after September 30, 1996 will be 'year 2000 compliant,' or will be modified to achieve 'year 2000 compliance' with minimal cost to the government."[442]

The language in the statute posed two difficulties: first, it did not set a deadline for compliance; and second, it did not provide a workable definition or clear standard for Year 2000 compliance.[443] Theoretically, the military departments could procure non-compliant IT without overstepping the statute's requirements, continually finding it "impracticable" to do otherwise during each successive procurement of non-compliant items. Furthermore, agencies could accept a vendor commitment to a compliance timetable that provided for Year 2000 compliance later than some critical point when the IT would have already experienced system failure or improperly processed date data. Fortunately, neither theoretical situation was given significant opportunity to develop as the legislative "loophole" for non-compliant IT procurements by the DoD was closed when the Year 2000 compliance standard was added to the FAR.[444]

The FAR Y2K provisions also provided the compliance definition that was lacking in this Act which required that acquired IT "ha[ve] the capabilities to process date and date-related data in 2000." The FAR's compliance definition is much more specific, requiring that the IT process accurately, effectively handle dates from either and both centuries, account for leap years, and perform specific types of processing accurately. Furthermore, the FAR's Y2K performance standard includes an exception provision for interoperability that is lacking here. The Act was directed in the right direction-- stemming the tide of government dollars for non-compliant IT--but needed more flesh on the bones to be a truly workable requirement.

---

[442] H.R. CONF. REP. NO. 724, 104th Cong., 2d Sess. 1996 (July 30, 1996), *reprinted in* 1996 U.S.C.A.N. 3130.

[443] Although the statute attempted to address the compliance problem by seeking to limit procurements to IT capable of processing date and date-related data in 2000, simple comparison of this standard to the definition which was added to FAR 39.002 will demonstrate the inefficacy of the requirement.

[444] 48 C.F.R. 39.002 and 39.106, added by interim rule by FAC 90-45, FAR Case 96-607, Item XIV, 62 FR 274, Jan 2, 1997, and adopted by final rule by FAC 97-01, FAR Case 96-607, Item XVII, 62 FR 44830, Aug 22, 1997.

The Act was one of Congress' earliest attempts to get a picture of where the DoD stood in relation to the Year 2000 Problem. Section 831 directed the Secretary of Defense to have the Chief Information Officers in each military department "assess all information technology within the[ir department] to determine the extent to which such technology has the capabilities to operate effectively."[445] Presumably the goal was to determine which systems were already capable of continuing effective operations into the next century and which would require conversion or replacement in order to avoid date-related problems. Additionally, δ831 required the Secretary to create a remedy plan from the assessment information, listing which major systems would be impacted by Y2K problems, any resulting national security concerns, and a prioritized estimate for achieving compliance. All in all, the Act was a step in the right direction, albeit somewhat later than is might have come.

2. *1998 General Appropriations Act*

The Treasury, Postal Service, and General Government Appropriations Act, 1998 included one section specifically targeting the Y2K Problem:

> None of the funds appropriated in this or any other Act shall be used to acquire information technologies which do not comply with part 39.106 (Year 2000 compliance) of the Federal Acquisition Regulation, unless an agency's Chief Information Officer determines that noncompliance with part 39.106 is necessary to the function and operation of the requesting agency or the acquisition is required by a signed contract with the agency in effect before the date of enactment of this Act. Any waiver granted by the Chief Information Officer shall be reported to the Office of Management and Budget, and copies shall be provided to Congress.[446]

This Act is broad-reaching, forcing government agencies using funds appropriated under this Act "or any other Act" as well. Importantly, the Act forces the Postal Service, which is not otherwise required to comply with the FAR when procuring goods and services, to comply with the FAR's Y2K compliance provisions when using

---

[445] Public Law 104-201, δ831(b) (HR 3230), 110 Stat. 2422 (September 23, 1996).
[446] Treasury, Postal Service, and General Government Appropriations Act, 1998, Pub. L. No. 105-61, δ631, 111 Stat. 1272, 1315 (1997).

B. Curtis

any appropriated funds to acquire IT. The Act does include an exception and a waiver provision. The agency CIO may make a determination that in order for his agency to continue functioning and operating, it will have to forego the FAR's Y2K compliance provisions in one or more of its acquisitions. The CIO's decision, termed a waiver, must be reported both to the Office of Management and Budget and the Congress. The increasing scrutiny on the Y2K topic will make the waiver provision a hard decision for any CIO.

The exception to the requirement to comply with FAR 39.106 is applicable when the agency had already entered a contract before the this Act was passed, and that contract requires an acquisition. Although the Act provides no explanatory language on this point, one could assume that Congress intended agencies to make every reasonable attempt to include Y2K provisions in existing contracts, and that this exception applies where those attempts have failed.[447] Furthermore, the Act would restrict an agency's ability to place additional orders under an indefinite quantity contract for non-compliant goods, at least once the agency had ordered the minimum quantity required under the contract. The Act represents another legislative attempt to close the remaining loopholes through which non-compliant products are entering the federal inventory.

3. OSD/C³I Memorandum

On December 15, 1997 the Acting CIO for the Department of Defense sent a letter to all Military Departments regarding IT acquisitions. The CIO went a step further than the General Appropriations Act had and required that the DoD acquire IT only if the equipment was Y2K compliant, regardless of when the department entered the contract for the items. Under this direction, to make an order under an existing contract, the item would have to be compliant, whether or not the minimum quantity had

---

[447] This would most likely occur in a commercial item contract where a changes clause would not have been included and the vendor was unwilling to agree to a modification that required Y2K compliance.

B. Curtis

already been ordered.[448]   As might be expected, the military departments were instructed to examine existing IT contracts to determine if Y2K compliance provisions needed to be added.   Finally, the letter required the Y2K compliance testing of a representative sampling of all IT acquired, whether the testing was performed by the contractor or the ordering agency.

4. *Secretary of Defense Memorandum*

The Secretary of Defense (SECDEF) began his August 7, 1998 memorandum by stating that the DoD was lagging behind in addressing the Y2K issues.[449] As part of his plan to make military leaders more accountable for Y2K solutions, SECDEF tasked specific senior leaders to develop plans to evaluate Y2K compliance status, and to report on readiness. He also required Program Executive Officers to report on the Y2K compliance status of all acquisition programs within their purview, including compliance action plans.   More importantly, SECDEF established an October 1, 1998 deadline, after which funds could not be obligated for mission-critical systems unless the Y2K compliance of those systems had been adequately addressed. The letter also made department and agency heads responsible for ensuring that "Funds are not obligated for any contract that is for information technology (IT) or national security system (NSS) that processes date-related information and that does not contain Y2K requirements specified in Section 39.106 of the Federal Acquisition Regulation" after October 1, 1998.[450] Unlike the 1998 General Appropriations Act, this edict came with no waiver

---

[448] Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998), *citing* Memorandum from Valletta, Acting Assistant Secretary of Defense for Command, Control, Communication and Intelligence, to the Secretaries of the Military Departments, et. al. (December 15, 1997).

[449] Memorandum from William Cohen, Secretary of Defense, to Secretaries of the Military Departments, et. al., *Year 2000 Compliance*, 7 August 1998, found at http://www.dtic.mil/c3i/y2k/secdefmemo.html, site visited on October 20, 1998.

[450] This portion of the letter was reiterated in a September 23, 1998 memorandum from OSD/ C^{3}I. *See* Memorandum from Arthur L. Money, Senior Civilian Official, Assistant Secretary of Defense for Command, Control, Communication and Intelligence, to the Secretaries of the Military Departments, et. al. (September 23, 1998), found at http://www.dtic.mil/c3i/y2k/policy/28sep1998.html, site visited on December 2, 1998.

B. Curtis

provisions or exceptions. In fact, the letter concluded with a rather stern warning of the steps that would follow if compliance remediation had not progressed sufficiently by December of 1998: "If we are still lagging behind, all further modification to software, except those needed for Y2K remediation, will be prohibited after January 1, 1999."

5. *Department of Agriculture*

In its regulations on Rural Utilities Service (RUS), the Department of Agriculture has standards for how RUS loans may be used to construct and outfit telephone facilities. For the RUS to loan money to finance telephone facilities, "[t]he materials and equipment must be year 2000 compliant,"[451] and the borrower's system must be economically feasible.[452] In order to be deemed economically feasible, so as to minimize the risk on the loan, the system must be Year 2000 compliant or the borrower must certify that it will be some reasonable time before December 31, 1999. For purposes of this program, "Year 2000 compliant means that product performance and function are not affected by dates before, during, and after the year 2000."[453] While this definition of Y2K compliance varies widely from that used in FAR 39.002, it probably provides adequate assurance for purposes of loan risk.

6. *Department of Labor*

In three separate Federal Register notices, the Department of Labor referenced Year 2000 compliance in regards to its Welfare to Work (WtW) grant program. Here, as with the Agriculture Department's loan funds, the agency wanted to ensure that limited grant money was used wisely. Regarding the allowability of costs under WtW grants, the notice stated that "[o]nly the costs of information technology that is 'year 2000 compliant' shall be allowable."[454] The second notice mandated that where WtW funds were used towards the purchase of IT that would be used after December 31, 1999, the

---

[451] 7 C.F.R. 1753.6(c).
[452] 7 C.F.R. 1735.22(e).
[453] 7 C.F.R. 1735.22(e).
[454] 62 FR 61588, November 18, 1997.

B. Curtis

acquired IT had to be Y2K compliant.[455] The third notice was an exact duplicate of the second notice.[456] All three notices defined Year 2000 compliant using language substantially similar to that used in FAR 39.002, although both definitions used the two-sentence "furthermore" structure from the interim rule that was revised out of the final FAR rule. The definition used here is not as important as in contracting because the element of liability risk is missing. Both borrower and lender are interested in getting equipment which will function properly for as long as possible. There is no vendor in this relationship who might desire to sell equipment regardless of its future reliability.

7. *Year 2000 Information Readiness and Disclosure Act*

This Act[457] is Congress' attempt to encourage entities to share information about the Year 2000 Problem by establishing limited protection from liability for Year 2000 readiness statements which are later found to have included false information.[458] The Act also provides a safe-haven from antitrust provisions for those who are willing to share Y2K information as part of their remediation efforts. Though this Act does not regulate government acquisition of commercial or non-commercial items, it is significant for this paper because it includes the first congressional Y2K definition: "The term 'year 2000 processing' means the processing (including calculating, comparing, sequencing, displaying, or storing), transmitting, or receiving of date data from, into, and between the 20th and 21st centuries, and during the years 1999 and 2000, and leap year calculations." The staff which drafted this language appears to have borrowed some from FAR 39.002, defining Year 2000 compliant, and FAR 2.101, defining information technology. Whatever the genesis of this language, it represents the first congressional definition of Year 2000 processing. It remains to be seen whether this language works its way into the FAR or other regulatory material.

---

[455] 62 FR 67902, December 30, 1997.
[456] 63 FR 18445, 18448, April 15, 1998.
[457] 15 USC § 1 (Note), Pub. L. No. 105-271 (1998).
[458] Year 2000 Law Report (BNA), Vol. 1, No. 7, 329 (October 1998).

B. Curtis

B. "YEAR 2000 COMPLIANCE," THE ULTIMATE STATUTORY TACK-ON

As the date rollover approaches, more and more acts will include a reference to the Year 2000 and the need for achieving compliance as quickly as possible. At this point in the game one might wonder how valuable such suggestions are: if a federally-controlled entity has not already completed its planning and completed a significant portion of its required remediation, the paragraph or so of Y2K comments plugged into an act will have little additional effect on that entity. One of the most common examples of Y2K compliance language that appears to have been "tacked on" to an act is the "Sense of the Congress on the Year 2000 Problem" which appears in a number of acts. As an example, the Technology Administration Act of 1998 includes such a section:

SEC. 5. SENSE OF THE CONGRESS ON THE YEAR 2000 PROBLEM.

With the year 2000 fast approaching, it is the sense of the Congress that the National Institute of Standards and Technology should--
(1) give high priority to correcting all 2-digit date-related problems in its computer systems to ensure that those systems continue to operate effectively in the year 2000 and beyond; and
(2) develop contingency plans for those systems that the Institute is unable to correct in time.[459]

Whenever the act involves an appropriation for a federal entity, it appears to include a section capturing the "Sense of the Congress on the Year 2000 Problem."[460]

C. PENDING OR POTENTIAL LEGISLATION

With the 105th Congress recently ended, pending litigation will have to be reintroduced at the next Congress. All the same, several members of Congress have indicated they may introduce legislation related to the Year 2000. Representative Christopher Cox (R-Calif.) states that he expects a bill similar to H.R. 4240, the Y2K

---

[459] Technology Administration Act, Pub. L. No. 105-309, 112 Stat. 2935 (1998).
[460] *See, i.e.* National Science Foundation Authorization Act of 1998--Appropriations, Pub. L. No. 105-207, 112 Stat. 869 (1998); Transportation Equity Act for the 21st Century, Pub. L. No. 105-178, 112 Stat. 107 (1998); FAA Research, Engineering, and Development Authorization Act of 1998, Pub. L. No. 105-155, 112 Stat. 5 (1998); Fire Administration Authorization for Fiscal Years 1998 and 1999, Pub. L. No. 105-108, 111 Stat. 2264 (1997).

B. Curtis

Liability and Antitrust Reform Act, to be introduced next session.[461] That bill, introduced on July 16, 1998 but not passed last session, was designed to limit corporate liability for Y2K failures and create a temporary antitrust exemption for companies to be able to share Y2K remediation efforts. Cox is interested in adding the liability limits so that Y2K litigation costs do not steal resources from ongoing remediation efforts. Representative Frank R. Mascara (D-Pa.) was one of a number of congressman irritated that the medical industry is not responding to government requests for compliance information on medical devices.[462] The Congressman suggested that legislation excluding non-reporting manufacturers from federal contracting may be the only effective means the federal government possesses to force manufacturers to provide the compliance information. Representative Constance Morella (R-Md.), Chair of the House Science Committee on Technology, projects that the next "Congress will have to explore the policy implications of creating safe harbors, caps on damages, consumer protection, and alternative dispute resolution (ADR) mechanisms" when considering Year 2000 liability and failure issues.[463] And, some have suggested that the federal government move to protect itself from Year 2000 litigation, much as some states have done and others are considering. The government could amend the Federal Tort Claims Act,[464] to limit the government's liability for its negligence under state substantive tort law; however, such actions implicate important policy considerations. The same is true of any actions to limit corporate liability for Y2K failures, ranging from products liability cases to breaches of the fiduciary duty to the corporation by its officers. These actions can been seen as corporate bailouts and might have the unintended result of slowing the pace of Y2K remediation when efforts should be pursued most vigorously.

---

[461] *Federal Spending Bill Includes $3.4B for Y2K Computer Problems at DOD, Other Agencies*, FEDERAL CONTRACTS REPORT, (BNA) Vol. 70, No. 15, 399, 406, October 26, 1998.
[462] Year 2000 Law Report (BNA), Vol. 1, No. 7, 329, 336-337 (October 1998).
[463] *Federal Spending Bill Includes $3.4B for Y2K Computer Problems at DOD, Other Agencies*, FEDERAL CONTRACTS REPORT, (BNA) Vol. 70, No. 15, 399, 406, October 26, 1998.
[464] 28 USC §§ 1346, 2671, 2680, *et. al.*

B. Curtis

VII. Conclusions and Recommendations

"Y2K is not a thing to fear, it's a thing to prepare for."[465]

A. Conclusions

The federal government, along with the commercial sector, has waited far too long to begin taking effective action on the Year 2000 Problem. Even though the United States may be further along the road to compliance than most of our technologically advanced global neighbors, current projections are that we will experience appreciable disruptions due to Year 2000 problems that have not been addressed adequately, if at all. Those disruptions are apt to be due, in large part, to the even less timely realization that embedded technology should have been addressed during the assessment and remediation planning for all other IT.

The GSA Year 2000 Warranty clauses and the FAR's Year 2000 compliance provisions established a government-wide compliance standard and were intended to put an end to non-compliant IT acquisitions. Those compliance measures present several shortcomings. The FAR compliance provisions are applicable to service contracts, whereas the GSA warranty does not--by its terms--readily apply to services. Both the GSA warranty and the FAR compliance definition use "to the extent" language to limit vendor responsibility to its own products. That "to the extent" language is subject to varying interpretations, one of which would require Y2K compliance *only* where IT is operated in combination with similarly compliant IT. Even under the intended reading, the interoperability exception places too much risk on the government; incompatible technical solutions will satisfy the definitional Y2K performance requirements but leave the government with equipment that cannot properly interface. Lastly, although the GSA warranty is stated in terms which encompass embedded IT (assuming the equipment is listed), the warranty is not

---

[465] Larry Burkett, founder and CEO of Christian Financial Concepts, found at http://www.cfcministry.org/library/Y2K/index.htm, site visited on October 23, 1998.

154 B. Curtis

required in any contracts. Even more problemsome, because the FAR excludes embedded IT from the definition of IT, the FAR's Y2K compliance provisions do not apply to embedded technology, regardless of the Y2K problems embedded technology may pose.

B. RECOMMENDATIONS

1. *Solicitations and Contracts*

Contracting officials should be careful to include Year 2000 compliance provisions when contracting for IT, rather than depending upon either the warranty of merchantability or the warranty of fitness for an intended purpose (assuming the commercial contract has not expressly disclaimed these warranties). Compliance may be required by including the GSA warranty, a reference to FAR 39.002, or specifications requiring Y2K compliance in all IT contracts. It is not terribly important whether the compliance provisions are implemented via contract specifications or a warranty clause. This is equally true whether the contract is for items that meet the FAR 2.101 definition of "information technology" or for items that contain embedded technology but do not fit the definition. The FAR Y2K compliance provisions do not preclude agencies from requiring embedded IT to be compliant; they simply do not demand such a requirement. Therefore, even in procurements for items that do not qualify as IT under the FAR definition of that term, solicitations and contracts should include Y2K compliance language if the item contains embedded _technology. Furthermore, unless the contracting office knows for a certainty that the item being procured will not contain potentially date-sensitive microprocessors, Y2K compliance should be included whether or not the item being acquired is used to process date data.

Where possible, the 4-digit year format should be selected as the technical solution, and this information included as a contract specification. A 4-digit year format is not a requirement for Y2K compliance. It is, however, the most practical long-term

155   B. Curtis

means for achieving the date formatting standardization that is more and more often required for world-wide data exchange. Whether the ANSI (year digits last) or ISO (year digits first) standard is selected, only one format should be used, and the time to make that decision is while the Herculean Y2K software conversions are being performed. The four-digit year date field will allow for accurate processing of date data through the next 8 centuries.

Lastly, vendors should be required to provide information about both the Y2K compliance of their product and the compliance of the basic items that normally interface with their product.[466] During early discussions between GSA and IT industry representatives, one common industry response to questions about product compliance was, "my product is compliant, but I cannot discuss the compliance of any other products; I do not know what you are going to use my product for."[467] Most commercial software packages come with information printed right on the side of the box, identifying minimum system requirements for successful operation of the software, such as the specific processor used, the clock speed of the processor, the operating system, memory requirements, and multi-media constraints. The prime author of the Y2K provisions opined that they probably should have included provision requiring vendors to supply this "short list" information about their products when responding to solicitations. Software and hardware vendors surely know—particularly with off-the-shelf commercial products--more than just whether their product is Y2K compliant. They also should have some idea of what other items are similarly compliant and will effectively operate with their product. Rather than allowing contractors to feign ignorance, we should require them to provide enough information about their product

---

[466] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 6, 1998). The information from this paragraph was developed from the discussion during this interview.
[467] This is not an actual quotation, but represents the type of answers received from one segment of the industry.

and the system requirements necessary for using that product so that our acquisition functions can determine whether the system, as a whole, will be Y2K compliant.

2. *FAR Revisions or Supplementation*

FAR staff should consider the development of a Year 2000 Warranty clause that specifically applies to IT service contracts. The IT service industry is not very interested in assuming the risk associated with guaranteeing their Y2K remediation work. But, service contractors should be willing to warrant their work against defects, much as software vendors are expected to warrant their products to be free from "bugs."

In responding to various public comments on the interim FAR Y2K compliance rule, the FAR IT Committee stated that they had suggested to the CIO Council's Year 2000 Subcommittee that non-regulatory guidance be developed to assist agencies with 1) implementing the FAR requirements;[468] 2) knowing what descriptive information to disclose to potential contractors regarding existing IT and when to make the disclosure;[469] and 3) understanding issues of interface, integration and interoperability.[470] Because no such guidance has been created or provided to date,[471] the FAR Councils should consider either revisiting their request with the CIO Council's Year 2000 Subcommittee, tasking the FAR IT Committee, or assembling some group specifically to produce this guidance. This type of implementation guidance would be greatly beneficial to those working in contracting offices, would provide more uniformity in the

---

[468] Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997), containing the FAR IT Committee Report on FAR Case 96-607 (found in Case File 96-607 at the FAR Secretariat), at 8.

[469] Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997), containing the FAR IT Committee Report on FAR Case 96-607 (found in Case File 96-607 at the FAR Secretariat), at 9.

[470] Memorandum from Lawrence Wolfe, Chairperson, FAR Information Technology Committee, to Ed Loeb, Chairman, Civilian Agency Acquisition Council, and Captain D.S. Parry, Director, Defense Acquisition Regulations Council (March 17, 1997), containing the FAR IT Committee Report on FAR Case 96-607 (found in Case File 96-607 at the FAR Secretariat), at 11.

[471] Telephonic interview with John Cornell, GSA Senior Assistant General Counsel, Personal Property Division (November 24, 1998).

B. Curtis

use of the various Y2K compliance measures, and would further promote the goal of ensuring the government does not augment the portion of the inventory that will cease to work properly in the Year 2000.

FAR 39.002 should be modified to more accurately and clearly represent the intent behind the definition, thereby eliminating inaccurate interpretations. The "to the extent" language should be removed and replaced with language that makes it clear that a vendor's product must be able to operate properly both in stand-alone mode and in combination with other equipment.

The suggestion in FAR 39.106 that agencies describe the existing IT resources that will be interfaced with the acquired IT, "as appropriate," should be made more directive. Procuring officials should be *required* to identify all IT that *may* be operated in combination with the acquired IT, whether or not that information technology is existing at the time of disclosure. If interfaces are planned and the technical requirements can be sufficiently determined, that information should be provided to the contractor. Moreover, the solicitation and contract should normally indicate the Y2K technical solution to be used in the acquired IT, or at least the solution employed in the interfacing IT. If contracting officials are required to provide this information, the dangers of including an exception clause for interoperability (like the one in FAR 39.002) would not be so great.

Finally, regulators should give serious consideration to expanding the application of the Year 2000 compliance requirements beyond the "information technology" currently covered. This could be done by revising the language used in FAR 39.002 and 39.106, or by altering the definition of IT in FAR 2.101. In any case, embedded technology is far too important a part of the Year 2000 issue to not be covered by the compliance requirements. And, FAR 39.106 should be adjusted so as to cover all IT that may be date-sensitive, regardless of whether it is used to process date/time data.

B. Curtis

3. *Legislative Solutions*

Unless the FAR Councils revise the FAR to address the compliance of embedded IT, Congress should consider either legislating such coverage or directing the Councils to make such revisions. Lawmakers should also consider whether Year 2000 compliance requirements should be limited to IT (embedded or otherwise), rather than requiring that all products--including everything from complex weapon systems to hair dryers--remain free from failures caused by internal date-related problems. Such a requirement would make irrelevant the question of whether the item processes date data; this scheme of Y2K compliance would provide coverage for items containing integrated multi-purpose chips that are sensitive to date data. Legislative pronouncements or implementing regulations could require date/time processing products to perform accurately and produce dependable results, regardless of the year, century or millennium of the processed dates, perhaps up to the year 9999. Under this scheme, products which do not process date data would also be adequately addressed: a requirement to function properly regardless of any date changes or date data would force contractors to address the date-handling for products containing date-sensitive chips, and create no new burden where the products was free of date-sensitive chips.

"[Y2K] is a severe, immense problem, and all anyone can do is plan for its solution. It will not go away and it will most assuredly make itself known on January 1, 2000."[472] It is not too late for the Federal Government to take actions to make changes in procurement policies that will affirmatively limit the Y2K impact on government operations and the public we serve.

---

[472] *Millennium Rollover: The Year 2000 Problem*, found at http://www.itl.nist.gov/div897/yr2000.htm, site visited on November 23, 1998, *quoting* NIST's Change Notice to FIPS 4-1, March 25, 1996.

B. Curtis

CASES

STATUTES

REGULATIONS

GOVERNMENT PUBLICATIONS

DAR Council, "Explanation of FAR Language," posted at
    http://www.govexec.com/dailyfed/0298/020598bt.htm, site visited on September 25, 1998----97, 104, 107
DOD YEAR 2000 MANAGEMENT PLAN, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND,
    CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I)), June 1998------------------- 16, 46, 47, 52, 53, 57, 134
GENERAL SERVICES ADMINISTRATION WHITE PAPER ON APPLICATION AND IMPLEMENTATION OF YEAR 2000
    FEDERAL ACQUISITION REGULATION GUIDANCE (August 1997)---
    ------------------------- 2, 34, 64, 65, 66, 72, 89, 95, 98, 102, 103, 105, 106, 107, 108, 110, 111, 113, 116, 120, 138
H.R. CONF. REP. NO. 724, 104th Cong., 2d Sess. 1996 (July 30, 1996) -------------------------------------- 146
H.R. Rep. No. 857, 104th Cong., 2d Sess. (1996)-- 5, 20, 21, 58, 60, 143
OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, AUDIT REPORT NO. 98-207, Year 2000
    Contract Language for Weapon Systems (September 22, 1998) ------------------------------------- 134, 135
REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON YEAR 2000 (April 1998) ------------------------ 17, 58
Richard Nunno, Analyst in Information Technology, Science Policy Research Division, Year 2000
    Computer Problem, Congressional Research Service, April 12, 1996---29
YEAR 2000 ASSESSMENT RATING, FINANCIAL INSTITUTION LETTERS (FIL-74-98), Federal Deposit Insurance
    Corporation, July 8, 1998 --36

JOURNALS

A. Monica, Year 2000 the Gathering Storm of Litigation of the "Millennium Bug," 13 ME. B.J. 184 (1998) ---
    --38, 118

PERIODICALS

Armstrong Williams, Millennium Bug's Painful Potential, WASH. TIMES, August 29, 1998 ----------------------28
Arnaud de Borchgrave, 'Millennium Bug' Battle a Case of Too Little, Too Late, THE WASH. TIMES, April 2,
    1998--57
Arthur Gross, IRS Associate Commissioner for Modernization (since resigned), congressional testimony
    quoted in IRS Countdown to Meltdown, INSIGHT, November 3, 1997 --41
Ashley Dunn, Y2K Bug: Problem for the Ages, WISCONSIN ST. J., at 1C, August 21, 1998 ----------10, 17, 91
Bill Burke, Second Y2K-like failure set to strike UNIX systems, BUSINESS TODAY, October 20, 1998 ------- 16
Bill Schadewald, Bull Market: A crash course in 'catastrophobia,' HOUSTON BUSINESS JOURNAL, June 1,
    1998--23
Bill Schadewald, Bull Market: Confessions of a Y2K Convert, HOUSTON BUSINESS JOURNAL, June 15,
    1998--24
Computer Sciences Gets U.S. Job, WALL ST. J., June 17, 1998 --62
David Lore, Will New Century Shut Off Utilities?, COLUMBUS DISPATCH, January 12, 1998--------------------43
Expenses Rising for Y2K Fix, CHICAGO TRIBUNE, October 21, 1998---63
Federal Spending Bill Includes $3.4B for Y2K Computer Problems at DOD, Other Agencies, FEDERAL
    CONTRACTS REPORT, (BNA) Vol. 70, No. 15, 399, 406, October 26, 1998 -------------------------------61, 153
GSA's New Recommended Year 2000 Warranty Clauses Balance Competing Interests, 38 GOV'T
    CONTRACTOR (Fed. Pubs. Inc.) 3 (September 18, 1996)-- 65, 66
Ian Davis, AUSTL. FIN. REV., May 23, 1998 ---62

Leyla Kokmen, *State Picks Logix for 2000 Work Four-Month-Old Firm Lands $1 Million Work*, DENV. POST, May 1, 1998 -- 55, 63

Peter de Jager, *Doomsday 2000*, COMPUTERWORLD, September 6, 1993 ------------------------- 8, 23, 27, 54, 59

Robert J. Kenney, Jr. and Michael F. Mason, *The 'Year 2000' Problem in Federal Procurement*, BRIEFING PAPERS, SECOND SERIES, No. 98-3 (1998) --------------------4, 64, 73, 80, 81, 85, 86, 92, 94, 95, 106, 128, 149

Robert L. Simison, *Year 2000 Problem Could Cost General Motors $500 Million*, THE WALL STREET JOURNAL INTERACTIVE EDITION, March 23, 1998--24

Sean Scully, *White House Doing too Little on Year-2000 'Crisis,' Hill Told*, WASH. TIMES, June 23, 1998 ---- --29, 34, 43, 58, 60, 143

Stephen Dinan, *Bug May Sting Computers Before 2000*, WASH. TIMES, September 8, 1998 --------11, 12, 14

Steve Hewitt (steve@ccmag.com), *Year 2000 Bug Part 1, The Challenge Ahead!* CHRISTIAN COMPUTING MAGAZINE, Volume 10 , Issue 9, Sep 1998 ---55, 116

Thomas Hoffman and Julia King, *Early Warning Signs of Y2K Glitches; 'Sneak previews' of January 2000 Already Cropping Up*, COMPUTERWORLD NEWS WIRE, August 24, 1998 --------- 24, 25, 26, 36, 37, 38, 39, 40

Timothy Dyck, *Y2K-Proofing Your Databases*, PC WEEK, October 19, 1998 ----------------------------- 22, 47

Where the Bug Will Bite, BUSINESS WEEK, Mar. 2, 1998--42

William Ulrich, *Microsoft Offers Little Year 2000 Help*, COMPUTER WORLD, Vol. 33, June 22, 1998 ---------21

Year 2000 Law Report (BNA), Vol. 1, No. 7, 329 (October 1998)-- 151

BOOKS

B. AUSTRIAN & T. PAGEL, MILLENNIUM MORASS (Montgomery Securities 1997) ----------------------------- 36, 54

DEAN A. MOREHOUS, JR., *Liability Issues and the Year 2000*, 21 December 1997, 18TH ANNUAL INSTITUTE OF COMPUTER LAW, PRACTISING LAW INSTITUTE, Volume 507 (Practising Law Institute 1998) -----36, 54, 56

EDWARD AND JENNIFER YOURDON, TIME BOMB 2000--WHAT THE YEAR 2000 COMPUTER CRISES MEANS TO YOU! (Prentice Hall PTR 1998) --11, 135, 136, 137

JOHN T. SOMA, COMPUTER TECHNOLOGY AND THE LAW (1983)-- 54, 61

THE HOLY BIBLE, Matthew 19:30 and Mark 10:31--31

VICTORIA NEUFELDT, EDITOR IN CHIEF, WEBSTER'S NEW WORLD DICTIONARY (Prentice Hall 3rd college ed. 1994) --84

WILLIAM MORRIS, EDITOR, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (Houghton Mifflin 1976) --- 84, 85

INTERNET SOURCES

Capers Jones, *Probabilities of Year 2000 Damages*, (February 26, 1998), found at http://www.year2000.com/archive/NFproby2k.html---23

China Sprays for Y2K Bugs, Reuters Special to CNET News.com, October 21, 1998, found at http://www.news.com/News/Item/0,4,27792,00.html ---31

De Jager, Peter, *It's a People Problem*, found at http://www.year2000.com/y2kpeople.html--------- 28, 54, 61

De Jager, Peter, *Moving to Zero*, September 1998, found at http://www.year2000.com/y2ktimeflies.html --- ---25

Dick Mills, *Another Myth, A Black Grid Can't Be Restarted*, August 14, 1998, found at http://www.y2ktimebomb.com/PP/RC/dm9832.htm---43

http://it.jobsearch.org/ --62

http://kraft.neog.com/careers/scoop/general.html --24

http://www.dir.state.tx.us/y2k/embedded/index.html-- 139

http://WWW.DODIG.OSD.MIL/audit/reports/index.html -- 134

http://www.itaa.org/definition.htm, site visited on June 23, 1998 ---57

http://www.itaa.org/Y2kadr1.htm, *citing Apocalypse Not*, TIME, June 1998 -----------------------------------56

http://www.itaa.org/y2kga.htm ---30, 58, 59

http://www.itl.nist.gov/div897/info2000.htm ---34

http://www.itpolicy.gsa.gov/library/yr2000/y201toc1.htm (August 1996)------------------------------- 66, 68

http://www.itpolicy.gsa.gov/mks/whitepr/y2kwpes.htm, site visited on June 23, 1998 --------------------------
--------------------------- 2, 34, 64, 65, 66, 72, 89, 95, 98, 102, 103, 105, 106, 107, 108, 110, 111, 113, 116, 120, 138
http://www.senate.gov/~bennett/pr609b98.html --42
http://www.y2ktimebomb.com/Bios/dmbio.htm --43
http://www.year2000.com/y2kbio.html --22
http://www.year2000.com/y2kbooks.html -- 4
http://www.year2000.com/y2kstock.html --44
Ian Galpin, *Year 2000 and ISO 8601 Notes,* last revised February 2, 1998, found at
 http://www.aegis1.demon.co.uk/y2k/y2kgen.htm--45
ITAA's Year 2000 Program, Year 2000 Law Suits (Filed & "Potential"), found at
 http://www.itaa.org/Y2Klaw.htm#Federal--38
Jay Golter and Paloma Hawry, *Circles of Risk,* found at
 http://www.year2000.com/archive/NFcirclesrisk.html ---22
Larry Burkett, founder and CEO of Christian Financial Concepts, found at
 http://www.cfcministry.org/library/Y2K/index.htm-- 154
Leap Years, Information Leaflet No. 48, Particle Physics and Astronomy Research Council, Royal
 Greenwich Observatory, April 17, 1996, found at
 http://www.ast.cam.ac.uk/pubinfo/leaflets/leapyear/leapyear.html --9, 10
Mark A. Frautschi, (frautsch@tmn.com), *Embedded Systems and the Year 2000 Problem (The OTHER
 Year 2000 Problem),* September 28, 1998 draft, found at http://www.tmn.com/~frautsch/y2k2.html --------
 --- 140, 141
*Millennia III Partners With Technology in Medicine, Inc. To Address Year 2000 Problems in Biomedical
 Devices* (June 17, 1998), found at http://www.year2000.com/releases/NFmillIII_6_17_1998.html ----- 137
Millennium Rollover: The Year 2000 Problem, found at http://www.itl.nist.gov/div897/yr2000.htm ------------
 -- 45, 46, 159
Rick Cowles, *Electric Utilities and Year 2000, Embedded Logic and Controls,* found at
 http://www.euy2k.com/embedded.htm -- 120
Robin Guenier, Task Force 2000 and former Government Millennium advisor, as quoted online at
 http://www.bbc.co.uk/education/disaster/bug.shtml--25, 26, 30, 136
*The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and
 Governments,* World Information Technology and Services Alliance White Paper, found at
 http://www.itaa.org/witsay2k.htm --- 17, 20
*The Titan Corporation Awarded State of Wyoming's Year 2000 Contract With Cap Gemini America as
 Subcontractor,* found at http://www.year2000.com/y2knews.html--- 55, 63
The Year AD 2000, Information Leaflet No. 52, Particle Physics and Astronomy Research Council, Royal
 Greenwich Observatory, May 23, 1996, found at
 http://www.ast.cam.ac.uk/pubinfo/leaflets/2000/2000.html---7, 9, 10
Year 2000 and Embedded Systems, found at http://www.iee.org.uk/2000risk/w-15.htm --------- 118, 119, 136

UNPUBLISHED MATERIALS

"Y2K ANNOUNCE: IQPC Houston Y2K Conf. Coverage," electronic mail received 22 June 1998 23:11:55
 -0500 (CDT) from The Year 2000 Information Center, http://www.year2000.com ----------------------------25
Christian Financial Concepts Y2K Position Paper (Updated September 23, 1998) --------------27, 41, 55, 118
Comments from Alex D. Tomaszczuk, Chair, Government Contracts Section, Federal Bar Association, in
 response to FAC 90-45 (March 3, 1997) --49, 101
Comments from Bert Concklin, President, Professional Services Council, March 3, 1997, in response to
 FAC 90-45 (March 3, 1997) -- 114
Comments from Gary Krump, Department of Veterans Affairs, Deputy Assistant Secretary for Acquisition
 and Materiel Management, in response to FAC 90-41 (October 7, 1996)------------------------ 121, 125, 126
Comments from Marc A. Pearl, General Counsel & Vice President, Government Affairs, ITAA, in response
 to FAC 90-45 (March 3, 1997) --- 113